
Welcome to Security in the Intelligence Community (IC)
Text Alternative



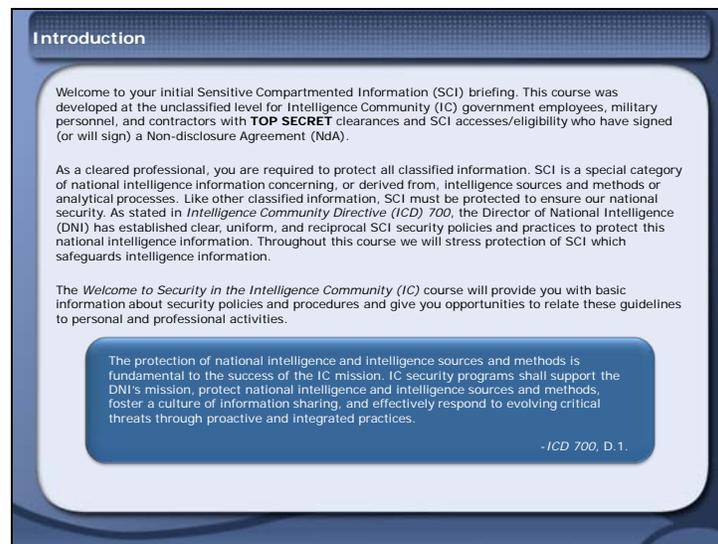
The Office of the Director of National Intelligence (ODNI)
Special Security Directorate
Community Services

Table of Contents

Welcome to Security in the Intelligence Community (IC)	3
Lesson 1: Welcome to Security in the IC Introduction	6
Topic 1.1: Defining the IC.....	7
Topic 1.2: Classification of Intelligence Information	24
Topic 1.3: Basic Security Overview	40
Topic 1.4: Threats to National Security	53
Lesson 2: Protecting SCI.....	71
Topic 2.1: Non-disclosure Agreements.....	72
Topic 2.2: Personnel Security (PERSEC)	82
Topic 2.3: Physical and Technical Security.....	95
Topic 2.4: Information Assurance and Cyber Security	107
Topic 2.5: Classification Management.....	119
Topic 2.6: Additional Responsibilities.....	135
Lesson 3: Our Changing Community.....	144
Topic 3.1: Evolution of the IC.....	145



Welcome to Security in the Intelligence Community (IC)

A blue-themed graphic with a dark blue header containing the word "Introduction" in white. The main body is light blue with rounded corners and contains three paragraphs of text. A dark blue call-out box at the bottom contains a quote. The entire graphic has a subtle grid pattern in the background.

Introduction

Welcome to your initial Sensitive Compartmented Information (SCI) briefing. This course was developed at the unclassified level for Intelligence Community (IC) government employees, military personnel, and contractors with **TOP SECRET** clearances and SCI accesses/eligibility who have signed (or will sign) a Non-disclosure Agreement (NDA).

As a cleared professional, you are required to protect all classified information. SCI is a special category of national intelligence information concerning, or derived from, intelligence sources and methods or analytical processes. Like other classified information, SCI must be protected to ensure our national security. As stated in *Intelligence Community Directive (ICD) 700*, the Director of National Intelligence (DNI) has established clear, uniform, and reciprocal SCI security policies and practices to protect this national intelligence information. Throughout this course we will stress protection of SCI which safeguards intelligence information.

The *Welcome to Security in the Intelligence Community (IC)* course will provide you with basic information about security policies and procedures and give you opportunities to relate these guidelines to personal and professional activities.

The protection of national intelligence and intelligence sources and methods is fundamental to the success of the IC mission. IC security programs shall support the DNI's mission, protect national intelligence and intelligence sources and methods, foster a culture of information sharing, and effectively respond to evolving critical threats through proactive and integrated practices.

-ICD 700, D.1.

Introduction

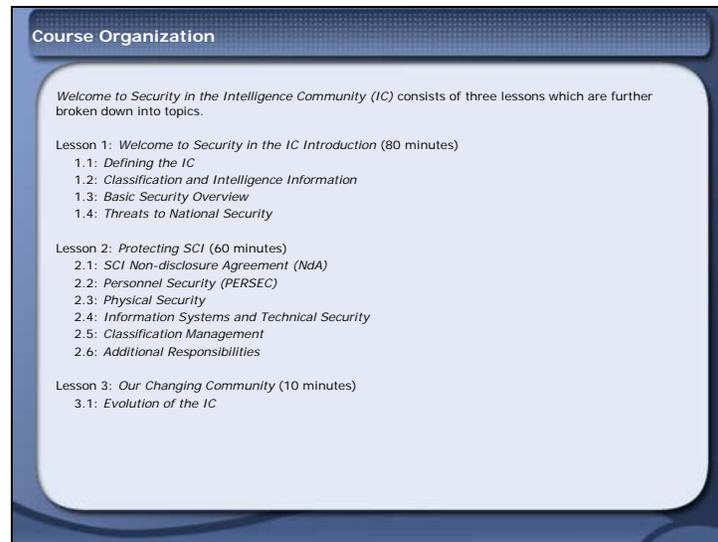
Welcome to your initial Sensitive Compartmented Information (SCI) briefing. This course was developed at the unclassified level for Intelligence Community (IC) government employees, military personnel, and contractors with **TOP SECRET** clearances and SCI accesses/eligibility who have signed (or will sign) a Non-disclosure Agreement (NDA).

As a cleared professional, you are required to protect all classified information. SCI is a special category of national intelligence information concerning, or derived from, intelligence sources and methods or analytical processes. Like other classified information, SCI must be protected to ensure our national security. As stated in *Intelligence Community Directive (ICD) 700*, the Director of National Intelligence (DNI) has established clear, uniform, and reciprocal SCI security policies and practices to protect this national intelligence information. Throughout this course we will stress protection of SCI which safeguards intelligence information.

The *Welcome to Security in the Intelligence Community (IC)* course will provide you with basic information about security policies and procedures and give you opportunities to relate these guidelines to personal and professional activities.

Call-Out Box: The protection of national intelligence and intelligence sources and methods is fundamental to the success of the IC mission. IC security programs shall support the DNI's mission, protect national intelligence and intelligence sources and methods, foster a culture of information sharing, and effectively respond to evolving critical threats through proactive and integrated practices.

-ICD 700, D.1.



Course Organization

Welcome to Security in the Intelligence Community (IC) consists of three lessons which are further broken down into topics.

Lesson 1: Welcome to Security in the IC Introduction (80 minutes)

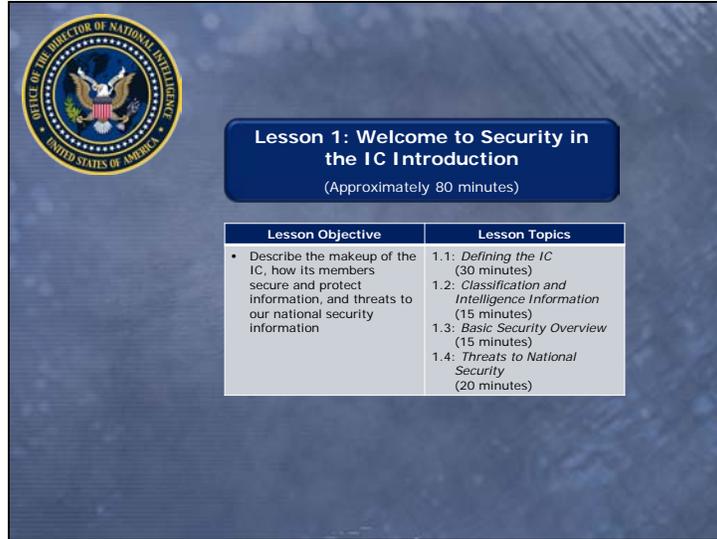
- 1.1: Defining the IC*
- 1.2: Classification and Intelligence Information*
- 1.3: Basic Security Overview*
- 1.4: Threats to National Security*

Lesson 2: Protecting SCI (60 minutes)

- 2.1: SCI Non-disclosure Agreement (NdA)*
- 2.2: Personnel Security (PERSEC)*
- 2.3: Physical Security*
- 2.4: Information Systems and Technical Security*
- 2.5: Classification Management*
- 2.6: Additional Responsibilities*

Lesson 3: Our Changing Community (10 minutes)

- 3.1: Evolution of the IC*



The slide features the Director of National Intelligence seal in the top left corner. The main title is "Lesson 1: Welcome to Security in the IC Introduction" with a subtitle "(Approximately 80 minutes)". Below this is a table with two columns: "Lesson Objective" and "Lesson Topics".

Lesson Objective	Lesson Topics
<ul style="list-style-type: none">Describe the makeup of the IC, how its members secure and protect information, and threats to our national security information	<ul style="list-style-type: none">1.1: <i>Defining the IC</i> (30 minutes)1.2: <i>Classification and Intelligence Information</i> (15 minutes)1.3: <i>Basic Security Overview</i> (15 minutes)1.4: <i>Threats to National Security</i> (20 minutes)

Lesson 1: Welcome to Security in the IC Introduction

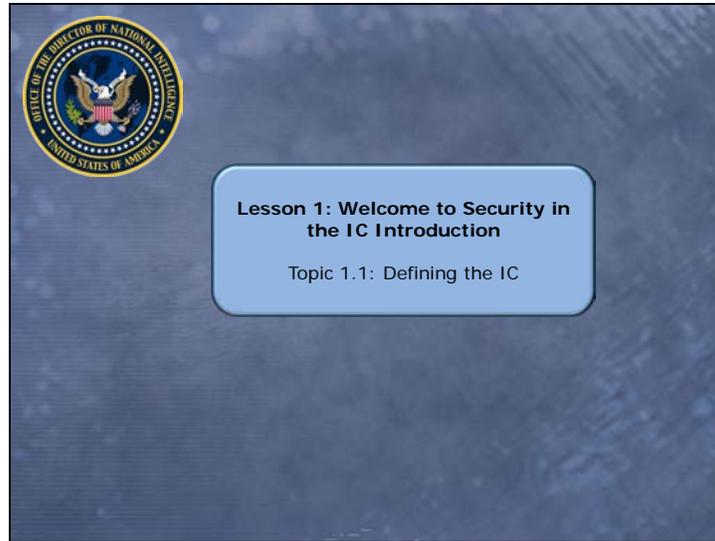
(Approximately 80 minutes)

Lesson Objective

- Describe the makeup of the IC, how its members secure and protect information, and threats to our national security information

Lesson Topics

- 1.1: *Defining the IC* (30 minutes)
- 1.2: *Classification and Intelligence Information* (15 minutes)
- 1.3: *Basic Security Overview* (15 minutes)
- 1.4: *Threats to National Security* (20 minutes)



Lesson 1: Welcome to Security in the IC Introduction

Topic 1.1: Defining the IC

Introduction and Objectives

The IC is made up of various organizations working independently and together to maintain foreign relations and protect national security. This topic will discuss the makeup of the IC, the categories into which the members fall, and their specific areas of responsibility. Additional partners will be described, as will their role in helping to strengthen relationships with foreign governments and non-National Intelligence Program (non-NIP) elements. You will also review the governing documents that define the IC.

Objectives

- Define the IC
- Describe the role of the DNI in the IC
- Identify the agencies and departments which comprise the IC
- Identify IC partners (e.g., Non-Title 50, Executive Office, private sector, non-NIP, etc.)
- Identify the key governing documents that define the IC and the capabilities of each IC element

The seal of the United States Intelligence Community is circular, featuring a central shield with a scale of justice and a sword, surrounded by a ring of stars and the text "UNITED STATES INTELLIGENCE COMMUNITY".

Introduction and Objectives

The IC is made up of various organizations working independently and together to maintain foreign relations and protect national security. This topic will discuss the makeup of the IC, the categories into which the members fall, and their specific areas of responsibility. Additional partners will be described, as will their role in helping to strengthen relationships with foreign governments and non-National Intelligence Program (non-NIP) elements. You will also review the governing documents that define the IC.

Objectives

- Define the IC
- Describe the role of the DNI in the IC
- Identify the agencies and departments which comprise the IC
- Identify IC partners (e.g., Non-Title 50, Executive Office, private sector, non-NIP, etc.)
- Identify the key governing documents that define the IC and the capabilities of each IC element

(Image Alt: U.S. IC seal)

Makeup of the IC

The IC is a federation of Executive Branch agencies and organizations that work independently and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States (U.S.).

Members of the IC perform the following functions:

- Collect information that allows the President, the National Security Council (NSC), the Secretaries of State and Defense, and other Executive Branch officials to perform their duties and responsibilities
- Produce and disseminate intelligence
- Collect information about, and conduct activities to protect against:
 - Intelligence activities directed against the U.S.
 - International terrorist and international narcotics activities
 - Other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents
- Conduct special activities (i.e., covert actions)
- Conduct administrative and support activities, within the U.S. and abroad, necessary for the performance of authorized activities
- Conduct other intelligence activities as directed by the President



NOTE!
For more information, see *An Overview of the Intelligence Community for the 111th Congress*.

Makeup of the IC

The IC is a federation of Executive Branch agencies and organizations that work independently and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States (U.S.).

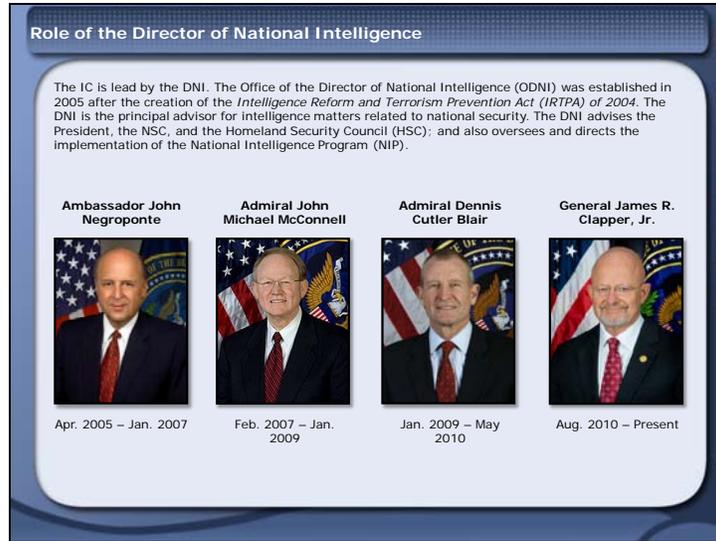
Members of the IC perform the following functions:

- Collect information that allows the President, the National Security Council (NSC), the Secretaries of State and Defense, and other Executive Branch officials to perform their duties and responsibilities
- Produce and disseminate intelligence
- Collect information about, and conduct activities to protect against:
 - Intelligence activities directed against the U.S.
 - International terrorist and international narcotics activities
 - Other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents
- Conduct special activities (i.e., covert actions)
- Conduct administrative and support activities, within the U.S. and abroad, necessary for the performance of authorized activities
- Conduct other intelligence activities as directed by the President

NOTE!

For more information, see *An Overview of the Intelligence Community for the 111th Congress*.

(Image Alt: Large seal of the Office of the Director of National Intelligence (ODNI) surrounded by small members' seals)



Role of the Director of National Intelligence

The IC is lead by the DNI. The Office of the Director of National Intelligence (ODNI) was established in 2005 after the creation of the *Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004*. The DNI is the principal advisor for intelligence matters related to national security. The DNI advises the President, the NSC, and the Homeland Security Council (HSC); and also oversees and directs the implementation of the National Intelligence Program (NIP).

(Image Alt: Gallery images of Ambassador John Negroponte; Admiral John Michael McConnell; Admiral Dennis Cutler Blair; and General James R. Clapper, Jr.)



Members of the IC

Introduction

There are sixteen different elements that comprise the IC. In general, these elements fall within the following categories:

- Independent
- Department of Defense (DoD)
- Departmental

Select the (+) by each seal to learn more about their role in the IC.

Additional information on all of the agencies can be found in the Course Resources. See *An Overview of the Intelligence Community for the 111th Congress*.

(Image Alt: Large Office of the Director of National Intelligence (ODNI) seal surrounded by small members' seals)

ODNI

Office of the Director of National Intelligence (ODNI)

The DNI serves as the head of the IC and is the principal advisor to the President, the NSC, and the HSC for intelligence matters related to national security. The President appoints the DNI with the advice and consent of the Senate. In addition to its staff elements, the ODNI comprises several components to include the National Counterterrorism Center (NCTC), the National Counterintelligence Executive (NCIX), and the National Counterproliferation Center (NCPC), each responsible for IC-wide coordination and support. The ODNI's focus is to promote its vision of a more integrated and collaborative IC.

CIA

Central Intelligence Agency (CIA)

As a member of the IC, the CIA is the largest producer of all-source national security intelligence for senior U.S. policymakers. The CIA's intelligence analysis on overseas developments feeds into decisions by policymakers and other senior decision makers in the national security and defense arenas. CIA is headquartered in McLean, Virginia.

DIA

Defense Intelligence Agency (DIA)

As a member of the IC, DIA collects, produces, and manages foreign military intelligence for policymakers and military commanders. It also has major activities at the Defense Intelligence Analysis Center (DIAC), on Bolling Air Force Base, Washington, DC; the Missile and Space Intelligence Center (MSIC), in Huntsville, AL; and the National Center for Medical Intelligence (NCMI), in Frederick, MD.

NGA

National Geospatial-Intelligence Agency (NGA)

As a member of the IC, the NGA collects and creates information about the Earth for navigation, national security, U.S. military operations, and humanitarian aid efforts. NGA, which is also part of the DoD, has facilities in Bethesda, MD (headquarters); St. Louis, MO; Reston, VA; and Washington, DC. It also has support teams worldwide.

NRO

National Reconnaissance Office (NRO)

The NRO was established in September 1961 as a classified agency of the DoD. The existence of the NRO and its mission of overhead reconnaissance were declassified in September 1992. As a member of the IC, the NRO is the "nation's eyes and ears in space." Headquartered in Chantilly, VA, the NRO is a joint organization engaged in the research and development, acquisition, launch, and operation of overhead reconnaissance systems necessary to meet the needs of the IC and the DoD.

NSA

National Security Agency (NSA)

As a member of the IC, the NSA is the U.S.' cryptologic organization, with responsibility for protecting U.S. national security information systems and collecting and disseminating foreign signals intelligence (SIGINT). Areas of expertise include cryptanalysis, cryptography, mathematics, computer science, and foreign language analysis. NSA is part of the DoD, and is staffed by a combination of civilian and military personnel. NSA's headquarters is at Ford Meade, MD.

U.S. Navy Intel.

United States Navy

Naval Intelligence (Navy Intel.)

As a member of the IC, the mission of Naval Intelligence is to support maritime operations worldwide and defend the U.S. Naval intelligence professionals are all members of the IC and are deployed throughout the Navy and the DoD.

USMC Intelligence Department
United States Marine Corps (USMC)
Intelligence Department

The Intelligence Department represents the Marine Corps within the IC on intelligence, counterintelligence, terrorism, classified information, security review, and cryptologic activities. The Marine Corps Director of Intelligence (DIRINT) is its principal intelligence staff officer, and is the service's functional manager for intelligence, counterintelligence, and cryptologic matters. Marine Corps Intelligence Activity (MCIA), in Suitland, MD, and Quantico, VA, is the USMC service production center.

USAF ISR
United States Air Force (USAF)
Intelligence, Surveillance, and Reconnaissance (ISR)

The Air Force ISR is the Air Force's main IC component. As a member of the IC, its mission is to organize, train, equip, and present assigned forces and capabilities to conduct intelligence, surveillance, and reconnaissance for combat commanders and the nation.

U.S. Army MI
United States Army
Army Military Intelligence (Army MI)

The Department of the Army's IC component is called Army Military Intelligence (Army MI). It is fully integrated into Army forces. Army MI's goal is to provide all-source intelligence that is relevant, useful, and timely to Army and other military personnel at all levels.

USCG
United States Coast Guard (USCG)

The Coast Guard is one of the five U.S. armed services and is a component of the Department of Homeland Security (DHS). As a member of the IC, the Coast Guard identifies and produces intelligence from raw information, assembles and analyzes multi-source operational intelligence, collects and analyzes communication signals using sophisticated computer technology, and provides input to and receives data from multiple computerized intelligence systems.

FBI NSB
Federal Bureau of Investigation (FBI)
National Security Branch (NSB)

The FBI, as an intelligence and law enforcement agency and a member of the IC, is responsible for understanding threats to our national security and penetrating national and transnational networks that have a desire and capability to harm the U.S. The FBI coordinates these efforts with its IC and law enforcement partners. It focuses on terrorist organizations, foreign intelligence services, weapons of mass destruction proliferators, and criminal enterprises. The FBI is headquartered in Washington, DC. It also has 56 field offices and more than 400 satellite

offices throughout the U.S. The FBI also has more than 50 international offices, known as “Legal Attachés,” in embassies worldwide.

DOS INR

Department of State (DOS)

Intelligence and Research (INR)

As an IC member, the INR provides all-source intelligence support to the Secretary of State and other State Department policymakers, including ambassadors, special negotiators, country directors, and desk officers. The INR is responsible for intelligence analysis, policy, and coordination of intelligence activities in support of diplomacy.

DHS I&A

Department of Homeland Security (DHS)

Office of Intelligence and Analysis (I&A)

As a member of the IC, the I&A is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the U.S. Although the following are not part of the IC, DHS also has intelligence activities in several components, including U.S. Immigration and Customs Enforcement, Customs and Border Protection, Transportation Security Administration, Secret Service, and Citizenship and Immigration Services.

Treasury OIA

Department of Treasury

Office of Intelligence and Analysis (OIA)

As a member of the IC, the Department of Treasury’s OIA supports the formulation of policy and execution of Treasury authorities by providing expert analysis and intelligence production on national security threats and focused intelligence support to Treasury officials on the full range of economic, political, and security issues.

DEA ONSI

Drug Enforcement Administration (DEA)

Office of National Security Intelligence (ONSI)

The DEA is responsible for enforcing the controlled substance laws and regulations of the U.S. As a member of the IC, DEA's ONSI, located at DEA Headquarters in Arlington, VA, facilitates intelligence coordination and information sharing with other members of the IC and homeland security elements. Its goal is to enhance the U.S.' efforts to reduce the supply of drugs, protect national security, and combat global terrorism.

DOE OIC

Department of Energy (DOE)

Office of Intelligence and Counterintelligence (OIC)

As a member of the IC, the DOE is responsible for U.S. energy policy and nuclear safety. DOE's IC component is the OIC, which provides timely technical intelligence analysis on all aspects of foreign nuclear weapons, nuclear materials, and energy issues worldwide.

Other Partners

The intelligence activities of the U.S. expand beyond these 16 elements of the IC. One of the enterprise objectives of the *National Intelligence Strategy (NIS)* drafted in 2009 was to "strengthen existing and establish new partnerships with foreign and domestic, public, and private entities to improve access to sources of information and intelligence, and ensure the appropriate dissemination of IC products and services."

This includes strengthening relationships with foreign government and non-NIP elements including:

- [Non-Title 50 Organizations](#)
- Executive Office of the President
- U.S. Legislative and Judicial Branches
- State, local, and tribal elements
- Private sector organizations

The ODNI is working to strengthen the IC's relationships with these partners to ensure that the IC's requirements for information and intelligence sharing are understood and met.



Other Partners

The intelligence activities of the U.S. expand beyond these 16 elements of the IC. One of the enterprise objectives of the *National Intelligence Strategy (NIS)* drafted in 2009 was to "strengthen existing and establish new partnerships with foreign and domestic, public, and private entities to improve access to sources of information and intelligence, and ensure the appropriate dissemination of IC products and services."

This includes strengthening relationships with foreign government and non-NIP elements including:

- [Non-Title 50 Organizations](#)
- Executive Office of the President
- U.S. Legislative and Judicial Branches
- State, local, and tribal elements
- Private sector organizations

The ODNI is working to strengthen the IC's relationships with these partners to ensure that the IC's requirements for information and intelligence sharing are understood and met.

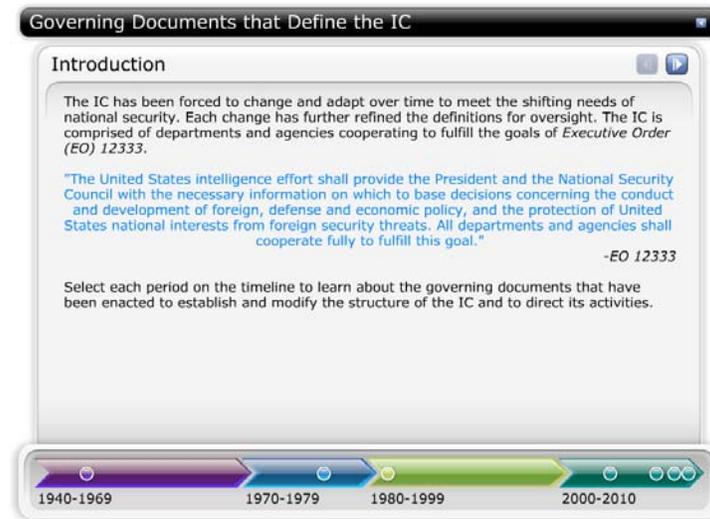
(Image Alt: Business professionals shaking hands in front of a group of other professionals; arrows connect various types of communication equipment in the background)

Non-Title 50 Organizations (pop-up)

Non-Title 50 Organizations are other U.S. government agencies outside of the IC including:

- U.S. Department of Agriculture (USDA)
- Department of Commerce
- Department of Health and Human Services
- Department of Labor
- Department of Transportation

- Department of Veterans Affairs
- National Aeronautics and Space Administration



Governing Documents that Define the IC

Introduction

The IC has been forced to change and adapt over time to meet the shifting needs of national security. Each change has further refined the definitions for oversight. The IC is comprised of departments and agencies cooperating to fulfill the goals of *Executive Order (EO) 12333*.

"The United States intelligence effort shall provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats. All departments and agencies shall cooperate fully to fulfill this goal."

-EO 12333

Select each period on the timeline to learn about the governing documents that have been enacted to establish and modify the structure of the IC and to direct its activities.

1940-1969

National Security Act of 1947

The *National Security Act of 1947*, which is still the legal foundation of the IC, mandated a major reorganization of the foreign policy and military establishments of the U.S. Government. It created many of the institutions that Presidents have found useful, including the following:

- NSC
- CIA

It merged the War and Navy Departments into a single DoD under the Secretary of Defense, who also directed the newly-created Department of the Air Force. Each of the three branches maintained their own service secretaries.

NOTE: The CIA grew out of the Office of Strategic Services (OSS), from the World War II (WWII) era, and also out of small, post-war, intelligence organizations. It served as the primary civilian, intelligence-gathering entity. Later, the DIA became the main military intelligence body.

1970-1979

EO 11905: U.S. Foreign Intelligence Activities (1976)

The purpose of *EO 11905*, signed by President Gerald R. Ford on February 18, 1976, was to establish policies to improve the quality of intelligence needed for national security, to clarify the authority and responsibilities of the intelligence departments and agencies, and to establish effective oversight to assure compliance with the law in the management and direction of intelligence agencies and departments of the national government.

EO 11905 defined the IC as the following organizations:

- CIA
- NSA
- DIA
- Special offices within the DoD for the collection of specialized intelligence through reconnaissance programs
- Intelligence elements within the following:
 - Military services
 - FBI
 - DOS
 - Department of the Treasury
 - Energy Research and Development Administration

1980-1999

EO 12333: U.S. Intelligence Activities (1981)

EO 12333, signed by President Ronald Reagan on December 4, 1981, established the IC. It defined the parameters of allowable intelligence activities and the roles and responsibilities of U.S. departments and agencies. It also prohibited the collection of intelligence against U.S. persons. *EO 12333* charged the IC with the following responsibilities:

- Collection of information needed by the President, the NSC, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities
- Production and dissemination of intelligence
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and/or narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons and their agents
- Special activities
- Administrative and support activities within the U.S. and abroad necessary for the performance of authorized activities
- Such other intelligence activities as the President may direct from time to time

2000-2010

Intelligence Reform and Terrorism Prevention Act (2004)

The *IRTPA* was signed by President George W. Bush on December 17, 2004. It was designed to reform the IC and the intelligence and intelligence-related activities of the U.S. Government, and for other purposes. It is divided into the following eight sections:

1. Reform of the IC
2. FBI
3. Security clearances
4. Transportation security
5. Border protection, immigration, and visa matters
6. Terrorism prevention
7. Implementation of 9/11 Commission recommendations
8. Other matters

The act also accomplished the following:

- Established the ODNI to manage the IC
- Established the NCTC
- Outlined information sharing responsibilities

National Intelligence Strategy (2005)

The *NIS*, released in 2005 by the DNI, is a product of the *IRTPA* that embodies a new approach to national intelligence and outlines the far-reaching reform of previous intelligence practices and arrangements. Its central theme is that "the time has come to integrate fully our efforts and to transform our institutions in the face of transnational threats menacing the United States at home and abroad." It defines strategic objectives that are mission and enterprise focused.

EO 12333: U.S. Intelligence Activities (2008)

EO 12333 was amended and signed by President George W. Bush on July 31, 2009. It advances and institutionalizes the reforms put into law by the *IRTPA* (2004) and provides a framework for the conduct of our intelligence activities. It continues to define the parameters of allowable intelligence activities and prohibits the collection of intelligence against U.S. persons. *EO 12333* directs the IC to produce timely, accurate, and insightful intelligence with special emphasis on international terrorism and the spread of weapons of mass destruction. In general, the amended EO addresses the following topics:

- Clarifies the responsibilities and strengthens the authority of the DNI
- Establishes policy on intelligence collection
- Defines the goal, direction, roles, and division of labor of each element in the IC
- Defines Heads of IC Elements (HICE) and Cognizant Security Authority (CSA)
- Maintains and strengthens protections for American Civil Liberties and privacy rights – it strengthens the protection of 1st amendment rights
- Retains the existing ban on assassination and the limitations on human experimentation

- Preserves and reinforces existing responsibilities of the IC members

National Intelligence Strategy (2009)

In August 2009, the DNI unveiled a new *NIS*, a blueprint that will drive the priorities for the 16 agencies of the IC for the next four years. This strategy:

- Lays out the strategic environment - challenges we face from other nations and non-state actors and those from global trends related to forces (i.e., economic, environmental, technological, pandemic)
- Describes mission and enterprise objectives
- Sets priorities and objectives
- Guides current and future decisions on budgets, acquisitions, and operations
- Defines four goals for the IC:
 1. Enable wise national security policies
 2. Support national security actions
 3. Deliver top-notch capabilities
 4. Operate as a team

Knowledge Check - Members of the IC
1 of 1

The DNI heads the IC which is comprised of 16 elements.
Select all of the organizations that are elements of the IC and then select SUBMIT.

- Defense Intelligence Agency (DIA)
- Customs and Border Protection (CBP)
- U.S. Department of Agriculture (USDA)
- Central Intelligence Agency (CIA)
- U.S. Coast Guard (USCG)
- U.S. Marine Corps (USMC)
- National Reconnaissance Office (NRO)
- Transportation Security Administration (TSA)
- Department of the Treasury
- Federal Bureau of Investigation (FBI)



SUBMIT

Knowledge Check - Members of the IC

1. The DNI heads the IC which is comprised of 16 elements.

Select all of the organizations that are elements of the IC and then select SUBMIT.

Choice
Defense Intelligence Agency (DIA)
Customs and Border Protection (CBP)
U.S. Department of Agriculture (USDA)
Central Intelligence Agency (CIA)
U.S. Coast Guard (USCG)
U.S. Marine Corps (USMC)
National Reconnaissance Office (NRO)
Transportation Security Administration (TSA)
Department of the Treasury
Federal Bureau of Investigation (FBI)

(Image Alt: Civilian and military professionals standing in front of the ODNI seal and various state labor seals.)

The following table reflects the correct answers.

Correct	Choice
X	Defense Intelligence Agency (DIA)
	Customs and Border Protection (CBP)
	U.S. Department of Agriculture (USDA)
X	Central Intelligence Agency (CIA)
X	U.S. Coast Guard (USCG)
X	U.S. Marine Corps (USMC)
X	National Reconnaissance Office (NRO)
	Transportation Security Administration (TSA)
X	Department of the Treasury
X	Federal Bureau of Investigation (FBI)

Feedback when correct:

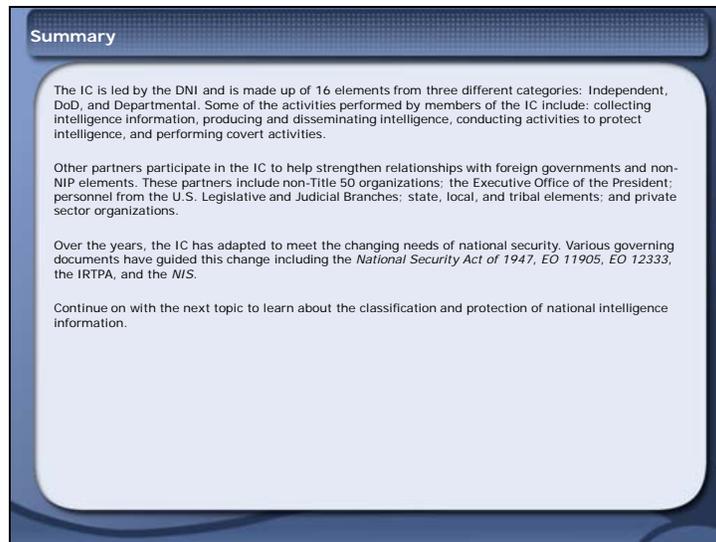
That's right! You selected the correct responses.

The IC is comprised of 16 elements. The DIA, CIA, USCG, USMC, NRO, Treasury, and FBI are amongst those elements. CBP, USDA, and TSA are not members of the IC, but they are non-Title 50 agencies.

Feedback when incorrect:

You did not select the correct responses.

The IC is comprised of 16 elements. The DIA, CIA, USCG, USMC, NRO, Treasury, and FBI are amongst those elements. CBP, USDA, and TSA are not members of the IC, but they are non-Title 50 agencies.



Summary

The IC is led by the DNI and is made up of 16 elements from three different categories: Independent, DoD, and Departmental. Some of the activities performed by members of the IC include: collecting intelligence information, producing and disseminating intelligence, conducting activities to protect intelligence, and performing covert activities.

Other partners participate in the IC to help strengthen relationships with foreign governments and non-NIP elements. These partners include non-Title 50 organizations; the Executive Office of the President; personnel from the U.S. Legislative and Judicial Branches; state, local, and tribal elements; and private sector organizations.

Over the years, the IC has adapted to meet the changing needs of national security. Various governing documents have guided this change including the *National Security Act of 1947*, *EO 11905*, *EO 12333*, the *IRTPA*, and the *NIS*.

Continue on with the next topic to learn about the classification and protection of national intelligence information.

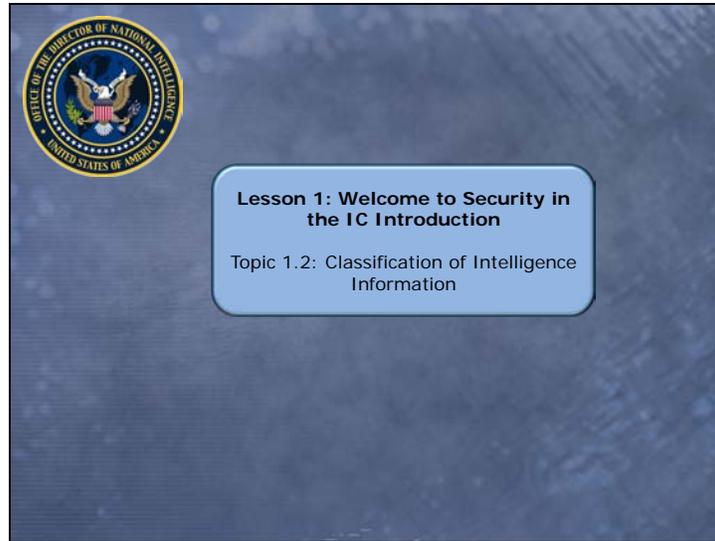
Summary

The IC is led by the DNI and is made up of 16 elements from three different categories: Independent, DoD, and Departmental. Some of the activities performed by members of the IC include: collecting intelligence information, producing and disseminating intelligence, conducting activities to protect intelligence, and performing covert activities.

Other partners participate in the IC to help strengthen relationships with foreign governments and non-NIP elements. These partners include non-Title 50 organizations; the Executive Office of the President; personnel from the U.S. Legislative and Judicial Branches; state, local, and tribal elements; and private sector organizations.

Over the years, the IC has adapted to meet the changing needs of national security. Various governing documents have guided this change including the *National Security Act of 1947*, *EO 11905*, *EO 12333*, the *IRTPA*, and the *NIS*.

Continue on with the next topic to learn about the classification and protection of national intelligence information.



Lesson 1: Welcome to Security in the IC Introduction

Topic 1.2: Classification of Intelligence Information

Introduction and Objectives

To safeguard classified national intelligence against unauthorized disclosure and to determine eligibility for access to classified national intelligence, IC entities rely on personnel clearances and access control programs. In order to access classified and controlled information, you must have the proper clearances and accesses.

In this topic you will explore the clearance levels and accesses, the distinction between them, and the importance of protecting SCI. You will also be introduced to the various intelligence collection disciplines used by members of the IC.

Objectives

- Define classified information
- Identify the three classification levels
- Define SCI
- Describe how SCI further restricts access to classified information
- Explain why we protect SCI
- Identify and describe the major collection disciplines
- Define a cleared professional
- Differentiate between clearances and access approvals



Introduction and Objectives

To safeguard classified national intelligence against unauthorized disclosure and to determine eligibility for access to classified national intelligence, IC entities rely on personnel clearances and access control programs. In order to access classified and controlled information, you must have the proper clearances and accesses.

In this topic you will explore the clearance levels and accesses, the distinction between them, and the importance of protecting SCI. You will also be introduced to the various intelligence collection disciplines used by members of the IC.

Objectives

- Define classified information
- Identify the three classification levels
- Define SCI
- Describe how SCI further restricts access to classified information
- Explain why we protect SCI
- Identify and describe the major collection disciplines
- Define a cleared professional
- Differentiate between clearances and access approvals

(Image Alt: Close-up of face with eye glasses, small members' seals are reflected in the eye glasses)

Classification Levels

The DNI is responsible for protecting classified national intelligence information and intelligence sources and methods from unauthorized disclosures. The classification level for intelligence information is based specifically on the determination that the unauthorized disclosure of the information reasonably could be expected to result in a specified level of damage to national security should information be disclosed to an unauthorized person. Classified national intelligence, for which only a classification level applies (no additional control markings are necessary), is referred to as "collateral" information.

Classification	Level of Damage
TOP SECRET (TS)	Exceptionally grave damage
SECRET (S)	Serious damage
CONFIDENTIAL (C)	Damage

Classification Levels

The DNI is responsible for protecting classified national intelligence information and intelligence sources and methods from unauthorized disclosures. The classification level for intelligence information is based specifically on the determination that the unauthorized disclosure of the information reasonably could be expected to result in a specified level of damage to national security should information be disclosed to an unauthorized person. Classified national intelligence, for which only a classification level applies (no additional control markings are necessary), is referred to as "collateral" information.

Classification – Level of Damage

TOP SECRET (TS) – Exceptionally grave damage

SECRET (S) – Serious damage

CONFIDENTIAL (C) – Damage

SCI Access

Access to intelligence information may be further controlled by compartmentation. Compartmentation is a term used to describe controlled access programs (i.e., SCI and Special Access Programs [SAP]). Access controls provide additional protection to the information because they are granted on a program-by-program basis with a formal need-to-know decision by the government Program Manager.

As a [cleared professional](#) who has signed a [Non-disclosure Agreement \(NdA\)](#), you have access to collateral national security information up to the level of your clearance (**TOP SECRET**, **SECRET**, or **CONFIDENTIAL**). In addition, you may be given access to some SCI programs depending on your position and mission need.

Clearances	Access Approvals
<ul style="list-style-type: none">• Granted by government agencies• Classifications<ul style="list-style-type: none">— TOP SECRET— SECRET— CONFIDENTIAL• Information is collateral• Informal need-to-know process	<ul style="list-style-type: none">• Must have the appropriate clearance level• Access to controlled programs granted by government program managers• Controlled access program data<ul style="list-style-type: none">— Classified at one of the three levels (i.e., TOP SECRET, SECRET, CONFIDENTIAL)— Further restricted through SCI accesses:<ul style="list-style-type: none">○ HCS – Human Intelligence (HUMINT) Control System○ KDK – KLONDIKE○ SI – Special Intelligence○ TK – Talent-Keyhole• Formal recognition of need-to-know process

SCI Access

Access to intelligence information may be further controlled by compartmentation. Compartmentation is a term used to describe controlled access programs (i.e., SCI and Special Access Programs [SAP]). Access controls provide additional protection to the information because they are granted on a program-by-program basis with a formal need-to-know decision by the government Program Manager.

As a [cleared professional](#) who has signed a [Non-disclosure Agreement \(NdA\)](#), you have access to collateral national security information up to the level of your clearance (**TOP SECRET**, **SECRET**, or **CONFIDENTIAL**). In addition, you may be given access to some SCI programs depending on your position and mission need.

Clearances

- Granted by government agencies
- Classifications
- **TOP SECRET**
- **SECRET**
- **CONFIDENTIAL**
- Information is collateral
- Informal need-to-know process

Access Approvals

- Must have the appropriate clearance level
- Access to controlled programs granted by government program managers
- Controlled access program data
- Classified at one of the three levels (i.e., **TOP SECRET**, **SECRET**, **CONFIDENTIAL**)
- Further restricted through SCI accesses:
 - HCS – Human Intelligence (HUMINT) Control System
 - KDK – KLONDIKE

- SI – Special Intelligence
- TK – Talent-Keyhole
- Formal recognition of need-to-know process

Cleared Professional (pop-up)

A cleared professional, as defined in *EO 13526*, is an authorized holder of classified national intelligence information. This means that the individual has met the following criteria:

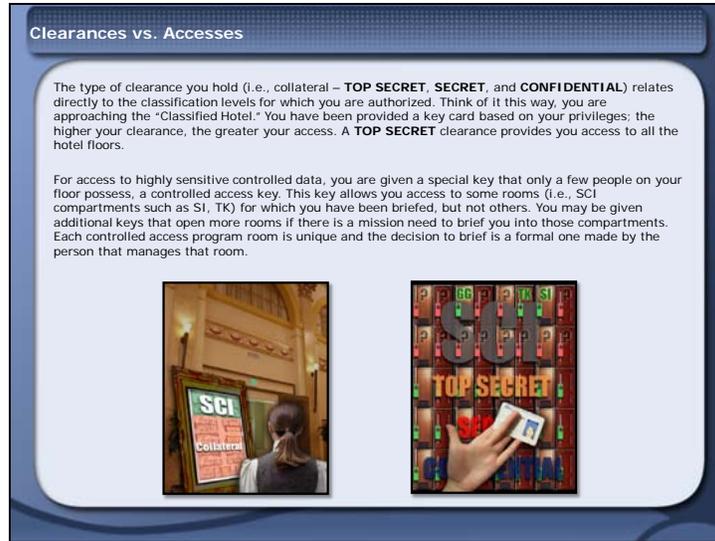
- Proved to be eligible by an agency head
- Signed an approved NdA
- Demonstrated a verified need to know for the information

Some agencies may also require the individual to successfully pass a polygraph.

Non-disclosure Agreement (NdA) (pop-up)

When you sign your NdA, you acknowledge that you understand:

- The lifelong commitment between you and the Government
- That it is a legal contract
- The importance and sensitivity of the intelligence information
- The pre-publication review requirement
- The need to protect against unauthorized disclosures
- That the information is government property
- The consequences if you breach the agreement



Clearances vs. Accesses

The type of clearance you hold (i.e., collateral – **TOP SECRET**, **SECRET**, and **CONFIDENTIAL**) relates directly to the classification levels for which you are authorized. Think of it this way, you are approaching the “Classified Hotel.” You have been provided a key card based on your privileges; the higher your clearance, the greater your access. A **TOP SECRET** clearance provides you access to all the hotel floors.

For access to highly sensitive controlled data, you are given a special key that only a few people on your floor possess, a controlled access key. This key allows you access to some rooms (i.e., SCI compartments such as SI, TK) for which you have been briefed, but not others. You may be given additional keys that open more rooms if there is a mission need to brief you into those compartments. Each controlled access program room is unique and the decision to brief is a formal one made by the person that manages that room.

(Image Alt: Woman in the lobby of a hotel with event board that reads “SCI Collateral”)

(Image Alt: Matrix of hotel doors labeled “SCI,” “**TOP SECRET**,” “**SECRET**,” and “**CONFIDENTIAL**”; hand holding identification card)

The Importance of Protecting Classified National Intelligence and SCI

As a cleared professional, you are accepting the responsibilities associated with protecting classified national intelligence from compromise or unauthorized disclosure. The WWII quote, "loose lips might sink ships," is a good rule of thumb to follow and is still relevant today.

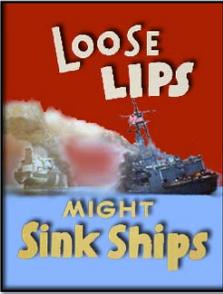
Compromise of classified intelligence sources and methods (SCI protected by access control systems) can result in loss of life and make us vulnerable to attack or exploitation.

We protect SCI because:

- SCI is the knowledge we have about non-U.S. governments and entities which provides an advantage to the U.S.
- SCI is a direct nexus to national security
- The loss or compromise of SCI is presumed to cause damage to national security
- Intelligence sources and methods take significant time and effort to develop

We protect SCI to:

- Enable the successful collection of accurate, timely, and unbiased foreign intelligence information
- Minimize denial and deception, or disruption to collection operations
- Sustain U.S. intelligence collection advantages



The Importance of Protecting Classified National Intelligence and SCI

As a cleared professional, you are accepting the responsibilities associated with protecting classified national intelligence from compromise or unauthorized disclosure. The WWII quote, "loose lips might sink ships," is a good rule of thumb to follow and is still relevant today.

Compromise of classified intelligence sources and methods (SCI protected by access control systems) can result in loss of life and make us vulnerable to attack or exploitation.

We protect SCI because:

- SCI is the knowledge we have about non-U.S. governments and entities which provides an advantage to the U.S.
- SCI is a direct nexus to national security
- The loss or compromise of SCI is presumed to cause damage to national security
- Intelligence sources and methods take significant time and effort to develop

We protect SCI to:

- Enable the successful collection of accurate, timely, and unbiased foreign intelligence information
- Minimize denial and deception, or disruption to collection operations
- Sustain U.S. intelligence collection advantages

(Image Alt: WWII era poster with three smoking battleships, label reads "Loose Lips Might Sink Ships")

Knowledge Check - Reasons to Protect SCI
1 of 2

National intelligence information is classified based on the determination that the unauthorized disclosure of the information reasonably could be expected to result in damage to national security should the information be disclosed to an unauthorized person. The level of damage to national security that would occur if the information were disclosed to an unauthorized person correlates directly to the classification level.

Match the level of damage to the correct classification and then select the Submit button.

TOP SECRET (TS) -- Select --

SECRET (S) -- Select --

CONFIDENTIAL (C) -- Select --

SUBMIT

Knowledge Check - Reasons to Protect SCI

1. National intelligence information is classified based on the determination that the unauthorized disclosure of the information reasonably could be expected to result in a specified level of damage to national security should the information be disclosed to an unauthorized person. The level of damage to national security that would occur if the information were disclosed to an unauthorized person correlates directly to the classification level.

Match the level of damage to the correct classification and then select the Submit button.

Clearance	Choice
TOP SECRET (TS)	Damage
SECRET (S)	Exceptionally grave damage
CONFIDENTIAL (C)	Serious damage

The following table reflects the correct answers.

Correct	Choice
TOP SECRET (TS)	Exceptionally grave damage
SECRET (S)	Serious damage
CONFIDENTIAL (C)	Damage

Feedback when correct:

That's right! You selected the correct responses.

The correct answers are:

TOP SECRET (TS) - Exceptionally grave damage

SECRET (S) - Serious damage

CONFIDENTIAL (C) - Damage

Feedback when incorrect:

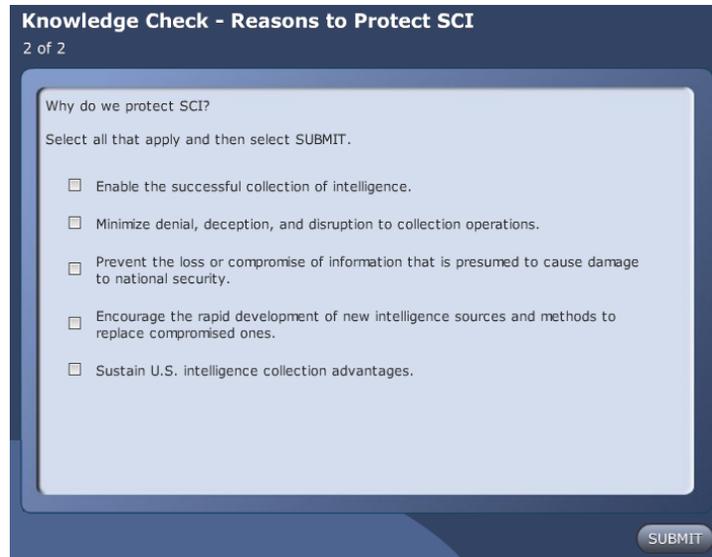
You did not select the correct responses.

The correct answers are:

TOP SECRET (TS) - Exceptionally grave damage

SECRET (S) - Serious damage

CONFIDENTIAL (C) - Damage



2. Why do we protect SCI?

Select all that apply and then select SUBMIT.

Choice
Enable the successful collection of intelligence.
Minimize denial, deception, and disruption to collection operations.
Prevent the loss or compromise of information that is presumed to cause damage to national security.
Encourage the rapid development of new intelligence sources and methods to replace compromised ones.
Sustain U.S. intelligence collection advantages.

The following table reflects the correct answers.

Correct	Choice
X	Enable the successful collection of intelligence.
X	Minimize denial, deception, and disruption to collection operations.
X	Prevent the loss or compromise of information that is presumed to cause damage to national security.
	Encourage the rapid development of new intelligence sources and methods to replace compromised ones.
X	Sustain U.S. intelligence collection advantages.

Feedback when correct:

That's right! You selected the correct responses.

You protect SCI to:

- Enable the successful collection of intelligence
- Minimize denial, deception, and disruption to collection operations
- Prevent the loss or compromise of information that is presumed to cause damage to national security
- Sustain U.S. intelligence collection advantages

Encouraging the rapid development of new intelligence sources and methods to replace compromised ones is incorrect. Intelligence sources and methods take a long time to develop and can be lost or compromised quickly. Once they are lost, they are difficult to replace.

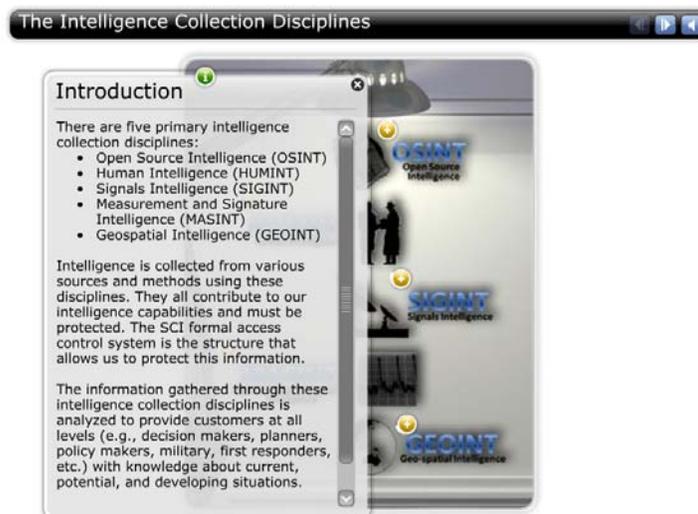
Feedback when incorrect:

You did not select the correct responses.

You protect SCI to:

- Enable the successful collection of intelligence
- Minimize denial, deception, and disruption to collection operations
- Prevent the loss or compromise of information that is presumed to cause damage to national security
- Sustain U.S. intelligence collection advantages

Encouraging the rapid development of new intelligence sources and methods to replace compromised ones is incorrect. Intelligence sources and methods take a long time to develop and can be lost or compromised quickly. Once they are lost, they are difficult to replace.



The Intelligence Collection Disciplines

Introduction

There are five primary intelligence collection disciplines:

- Open Source Intelligence (OSINT)
- Human Intelligence (HUMINT)
- Signals Intelligence (SIGINT)
- Measurement and Signature Intelligence (MASINT)
- Geospatial Intelligence (GEOINT)

Intelligence is collected from various sources and methods using these disciplines. They all contribute to our intelligence capabilities and must be protected. The SCI formal access control system is the structure that allows us to protect this information.

The information gathered through these intelligence collection disciplines is analyzed to provide customers at all levels (e.g., decision makers, planners, policy makers, military, first responders, etc.) with knowledge about current, potential, and developing situations.

Select each INT (+) to learn more about it.

(Image Alt: The five primary intelligence collection disciplines: OSINT, HUMINT, SIGINT, MASINT, and GEOINT)

OSINT

Open Source Intelligence (OSINT) is information that is available through public sources such as the following:

- Press/media (e.g., journals, newspapers, etc.)
- Internet (e.g., websites, blogs, etc.)
- Speeches
- Libraries

- Conferences
- Television

NOTE: Not all OSINT is easily accessible; for example, it may be in a foreign language.

In the IC there are several agencies that collect OSINT, including the following:

- Open Source Center, ODNI
- DIA
- FBI

HUMINT

Human Intelligence (HUMINT) is intelligence gathering by means of human contact. HUMINT can be overtly or covertly collected.

The National Clandestine Service (NCS) of the CIA is responsible for foreign HUMINT operations.

SIGINT

Signals Intelligence (SIGINT) is the collection of both verbal and non-verbal electronic emissions by other than the intended recipients. SIGINT is protected within the Communications Intelligence (COMINT) control system.

NSA is the executive agent for SIGINT collection.

MASINT

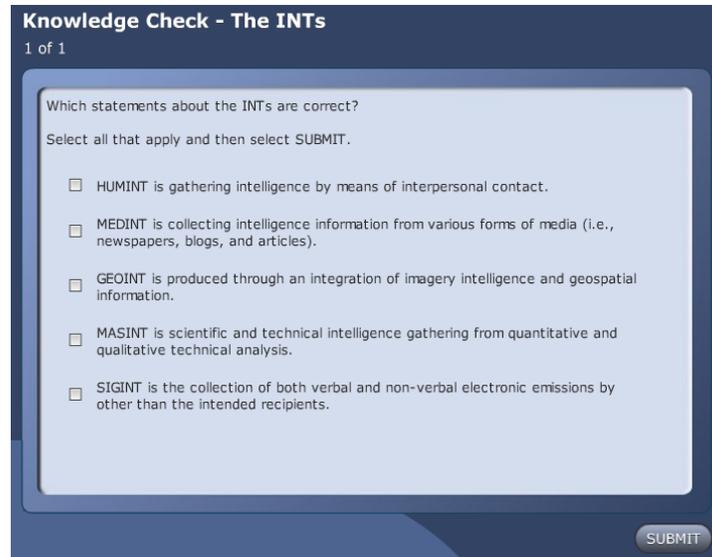
Measurement and Signature Intelligence (MASINT) is the collection of scientific and technical intelligence from quantitative and qualitative technical analysis. MASINT is science intensive and it straddles traditional intelligence disciplines.

DIA is the executive agent of MASINT.

GEOINT

Geospatial Intelligence (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities of the Earth. GEOINT consists of imagery, imagery intelligence, and geospatial (e.g., mapping, geodesy, etc.) information.

NGA is the executive agent of GEOINT.



Knowledge Check - The INTs

1. Which statements about the INTs are correct?

Select all that apply and then select SUBMIT.

Choice
HUMINT is gathering intelligence by means of interpersonal contact.
MEDINT is collecting intelligence information from various forms of media (i.e., newspapers, blogs, and articles).
GEOINT is produced through an integration of imagery intelligence and geospatial information.
MASINT is scientific and technical intelligence gathering from quantitative and qualitative technical analysis.
SIGINT is the collection of both verbal and non-verbal electronic emissions by other than the intended recipients.

The following table reflects the correct answers.

Correct	Choice
X	HUMINT is gathering intelligence by means of interpersonal contact.
	MEDINT is collecting intelligence information from various forms of media (i.e., newspapers, blogs, and articles).
X	GEOINT is produced through an integration of imagery intelligence and geospatial information.
X	MASINT is scientific and technical intelligence gathering from quantitative and qualitative technical analysis.
X	SIGINT is the collection of both verbal and non-verbal electronic emissions by other than the intended recipients.

Feedback when correct:

That's right! You selected the correct responses.

The following are correct collection disciplines:

- HUMINT is gathering intelligence by means of interpersonal contact
- GEOINT is produced through an integration of imagery intelligence and geospatial information
- MASINT is scientific and technical intelligence gathering from quantitative and qualitative technical analysis
- SIGINT is the collection of both verbal and non-verbal electronic emissions by other than the intended recipients

The collection of media is included in OSINT.

Feedback when incorrect:

You did not select the correct responses.

The following are correct collection disciplines:

- HUMINT is gathering intelligence by means of interpersonal contact
- GEOINT is produced through an integration of imagery intelligence and geospatial information
- MASINT is scientific and technical intelligence gathering from quantitative and qualitative technical analysis
- SIGINT is the collection of both verbal and non-verbal electronic emissions by other than the intended recipients

The collection of media is included in OSINT.

Summary

The three different classification levels for national intelligence information are **TOP SECRET**, **SECRET**, and **CONFIDENTIAL**. Information is classified based on the level of damage to national security should an unauthorized disclosure occur. Additional access controls provide supplemental safeguards for SCI data and are implemented on a program-by-program basis. It is essential that you, as a cleared professional, fulfill your promise to protect SCI. Compromise of this information can result in loss of life and make the U.S. and our allies vulnerable to attack or exploitation.

Members of the IC employ various methods to collect intelligence information. The five primary intelligence collection disciplines are: OSINT, HUMINT, SIGINT, MASINT, and GEOINT.

In the next topic you will be introduced to the four key security protection methods and the Operations Security (OPSEC) process by which you can effectively protect security information.

A collage of classified documents, an SCI folder, and communications and reconnaissance equipment. The collage includes a folder labeled 'Sensitive Compartmented Information', several documents with classification markings like 'TOP SECRET', 'SECRET', and 'CONFIDENTIAL', and images of a satellite, an aircraft, and a radar dish.

Summary

The three different classification levels for national intelligence information are **TOP SECRET**, **SECRET**, and **CONFIDENTIAL**. Information is classified based on the level of damage to national security should an unauthorized disclosure occur. Additional access controls provide supplemental safeguards for SCI data and are implemented on a program-by-program basis. It is essential that you, as a cleared professional, fulfill your promise to protect SCI. Compromise of this information can result in loss of life and make the U.S. and our allies vulnerable to attack or exploitation.

Members of the IC employ various methods to collect intelligence information. The five primary intelligence collection disciplines are: OSINT, HUMINT, SIGINT, MASINT, and GEOINT.

In the next topic you will be introduced to the four key security protection methods and the Operations Security (OPSEC) process by which you can effectively protect security information.

(Image Alt: Collage of classified documents, an SCI folder, and communications and reconnaissance equipment)



Lesson 1: Welcome to Security in the IC Introduction

Topic 1.3: Basic Security Overview

Introduction and Objectives

Maintaining the safety and integrity of SCI is a team effort. Security is a combination of processes and procedures enacted everyday to help you and your cleared coworkers, protect SCI. Learning the basics of security, what it protects, and how it protects, will enable you to work responsibly and effectively in a secure environment. Security is only as good as its weakest link and works only as long as cleared professionals do not become complacent.

In this topic you will explore the methods used to protect classified information, the IC assets that they protect, and how they are protected.

Objectives

- Identify security protection methods
- Describe what each security method protects
- Identify how OPSEC supports you in the execution of your security responsibilities
- Identify the various components of an effective security program



Introduction and Objectives

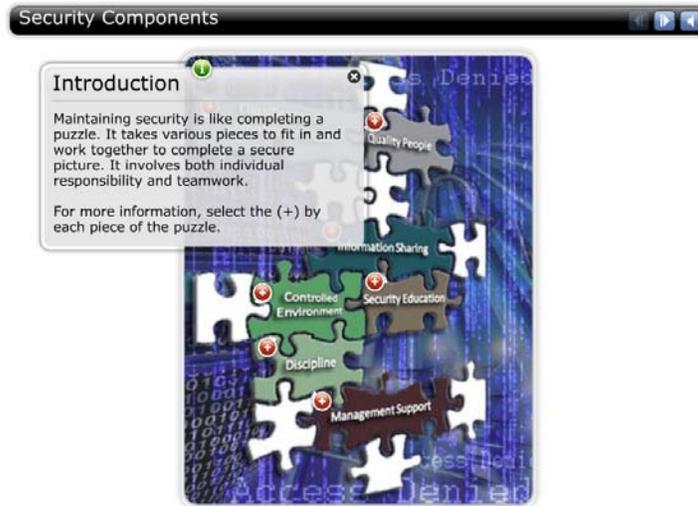
Maintaining the safety and integrity of SCI is a team effort. Security is a combination of processes and procedures enacted everyday to help you and your cleared coworkers, protect SCI. Learning the basics of security, what it protects, and how it protects, will enable you to work responsibly and effectively in a secure environment. Security is only as good as its weakest link and works only as long as cleared professionals do not become complacent.

In this topic you will explore the methods used to protect classified information, the IC assets that they protect, and how they are protected.

Objectives

- Identify security protection methods
- Describe what each security method protects
- Identify how OPSEC supports you in the execution of your security responsibilities
- Identify the various components of an effective security program

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification management surrounded by Operations Security)



Security Components

Introduction

Maintaining security is like completing a puzzle. It takes various pieces to fit in and work together to complete a secure picture. It involves both individual responsibility and teamwork.

For more information, select the (+) by each piece of the puzzle.

(Image Alt: Puzzle pieces labeled with Quality People, Security Education, Controlled Environment, Classification and Compartmentation, Discipline, Information Sharing, and Management Support)

Classification & Compartmentation

Classification occurs when an Original Classification Authority (OCA) determines the necessity of removing information from the public domain and protecting it as national security information in accordance with established laws and EOs.

Compartmentation applies further restrictions to the dissemination of classified information by granting access, through a formal need-to-know process, only to those who need it.

Quality People

People who are loyal, reliable, and trustworthy.

Information Sharing

After September 11, 2001 (9/11), the DNI provided guidance to improve information sharing across the IC. This guidance stated that information must be shared and protected. This entails changing the need-to-know philosophy with a responsibility-to-provide philosophy.

- Responsibility-to-provide reflects the information sharing requirement
- Need-to-know reflects the protection requirement

As a cleared professional, when making a determination about whether to share information, you need to ask yourself “Why shouldn’t I share this information?”

Controlled Environment

Security controls access to your work environment and to classified information.

Security Education

A strong security education program that presents the rules, the responsibilities of the cleared professionals who implement them, and the impact to national security if the rules are not followed.

Discipline

Personnel consistently act in accordance with established rules and processes.

Management Support

Having management believe in the importance of security is essential so that they may ensure that:

- Resources are available for proper security implementation
- Their workforce understands the importance of security
- Their workforce has the knowledge to implement security procedures



Key Security Methods

Introduction

The government has a responsibility to protect its assets. In fact, we all have a responsibility to protect these assets. The compromise of any one asset can have a negative effect on another.

Security methods are in place to protect information (SCI). They also protect the following assets:

- People
- Systems (i.e., information systems and networks)
- Facilities and property

They are in place to defend against:

- Espionage
- Terrorism
- Sabotage
- Damage
- Theft

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification management surrounded by Operations Security)

Personnel Security (PERSEC)

Personnel security (PERSEC) is the security method that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information.

Authoritative Source

- ICD 704 (formerly Director of Central Intelligence Directive [DCID] 6/4)

Physical & Technical Security

Physical security is the method designed to prevent unauthorized physical access to, and detect attempts at unauthorized access to the following:

- Information
- Facilities
- Equipment
- Materials

Technical security is the method designed to:

- Prevent unauthorized access to information contained on or in communication technologies
- Prevent the compromise of classified information, through compromising emanations and other technical hazards, using TEMPEST, Technical Security Countermeasures (TSCM), and telecommunications security

Authoritative Sources

- Physical Security - *ICD 705* (formerly *DCID 6/9*)
- Technical Security
- Committee on National Security Systems (CNSS) 7000
- CNSS 500
- ICD 702

Information Assurance & Cyber Security

Information assurance and cyber security are the security methods that develop and implement policies and procedures for Information Technology (IT) systems security, risk management, certification, and accreditation. These protective measures consider economic and operational costs against mission requirements.

Authoritative Source

- ICD 503 (formerly DCID 6/3)

Classification Management

Classification management is the security method that provides the IC procedures for protecting intelligence information and sources and methods while ensuring that information is available without delay or unnecessary restrictions. Classification management provides guidance on the proper classification, marking, handling, safeguarding, and declassification of classified information.

Authoritative Sources

- EO 13526
- ICD 710 (formerly DCID 6/6)
- 32 Code of Federal Regulations (CFR) Parts 2001 and 2003, Classified National Security Information; Final Rule

Operations Security

OPSEC is the process of identifying unclassified activities and information and evaluating the potential those might have in revealing classified national intelligence information. Once these situations are identified, commonsense and cost-effective countermeasures can be put in place to mitigate the risk of compromise.

The following are examples of situations in which unclassified evidence can provide adversaries with information about our classified activities:

- Wearing your badge outside of the office (because it can indicate where you work)
- Talking about your work in social settings
- Carrying classified materials (e.g., lock bag)
- Having a high-security/spin dial lock on the outside door of a commercial office building
- Using your work email address when anonymity may be important

For more information on OPSEC, access the Interagency OPSEC Support Staff website (www.iooss.gov) from the Course Resources.

CAUTION!
When completing your day-to-day activities, you should ask yourself, “What might this action reveal about my classified work?”



Operations Security

OPSEC is the process of identifying unclassified activities and information and evaluating the potential those might have in revealing classified national intelligence information. Once these situations are identified, commonsense and cost-effective countermeasures can be put in place to mitigate the risk of compromise.

The following are examples of situations in which unclassified evidence can provide adversaries with information about our classified activities:

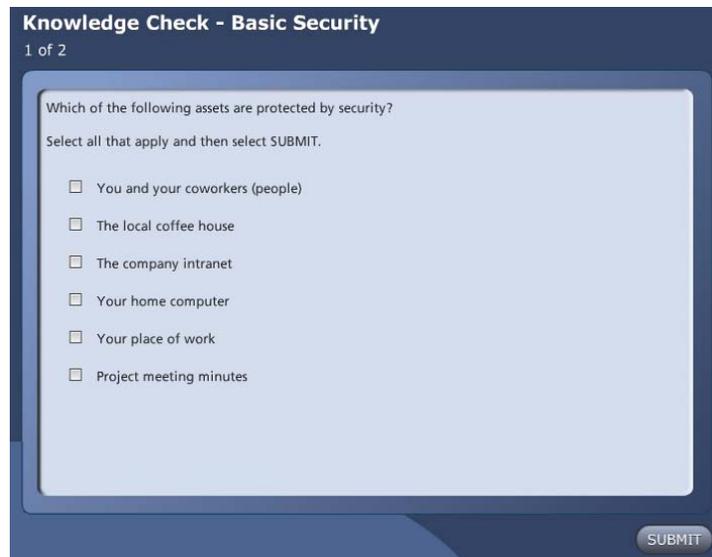
- Wearing your badge outside of the office (because it can indicate where you work)
- Talking about your work in social settings
- Carrying classified materials (e.g., lock bag)
- Having a high-security/spin dial lock on the outside door of a commercial office building
- Using your work email address when anonymity may be important

For more information on OPSEC, access the Interagency OPSEC Support Staff website (www.iooss.gov) from the Course Resources.

CAUTION!

When completing your day-to-day activities, you should ask yourself, “What might this action reveal about my classified work?”

(Image Alt: Collage of various OPSEC components)



Knowledge Check - Basic Security

1. Which of the following assets are protected by security?

Select all that apply and then select SUBMIT.

Choice
You and your coworkers (people)
The local coffee house
The company intranet
Your home computer
Your place of work
Project meeting minutes

The following table reflects the correct answers.

Correct	Choice
X	You and your coworkers (people)
	The local coffee house
X	The company intranet
	Your home computer
X	Your place of work
X	Project meeting minutes

Feedback when correct:

That's right! You selected the correct responses.

The following assets are protected by security:

- You and your coworkers (people)
- The company intranet
- Your place of work
- Project meeting minutes - may contain sensitive or proprietary project information

The following are incorrect:

- The local coffee house - this is a public place
- Your home computer - you would not use your home computer for classified work

Feedback when incorrect:

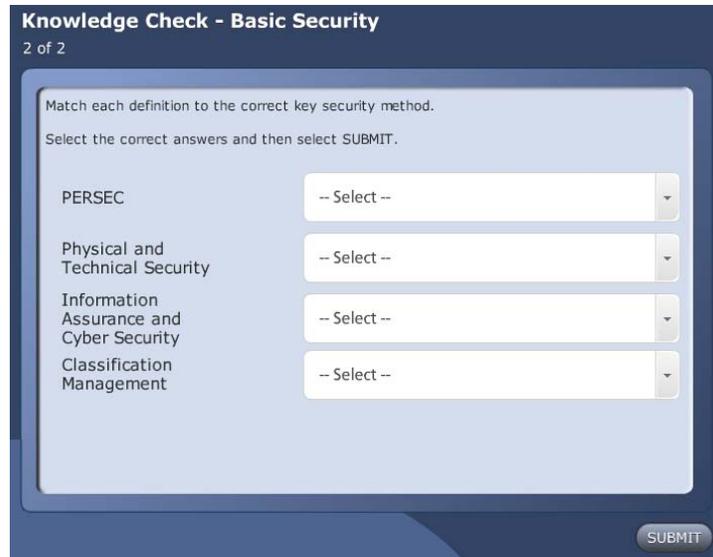
You did not select the correct responses.

The following assets are protected by security:

- You and your coworkers (people)
- The company intranet
- Your place of work
- Project meeting minutes - may contain sensitive or proprietary project information

The following are incorrect:

- The local coffee house - this is a public place
- Your home computer - you would not use your home computer for classified work



2. Match each definition to the correct key security method.

Select the correct answers and then select SUBMIT.

Key Security Method	Definition
PERSEC	Assesses the loyalty reliability, and trustworthiness of individuals holding or requesting a clearance.
Physical and Technical Security	Develops and implements policies and procedures for IT systems security risk management, certification, and accreditation.
Information Assurance and Cyber Security	Prevents unauthorized access to, and detects attempts at, unauthorized access to physical or communication technologies.
Classification Management	Provides the IC procedures for protecting intelligence information and sources and methods while maintaining its availability.

The following table reflects the correct answers.

Correct	Choice
PERSEC	Assesses the loyalty reliability, and trustworthiness of individuals holding or requesting a clearance.
Physical and Technical Security	Prevents unauthorized access to, and detects attempts at, unauthorized access to physical or communication technologies.
Information Assurance and Cyber Security	Develops and implements policies and procedures for IT systems security risk management, certification, and accreditation.
Classification Management	Provides the IC procedures for protecting intelligence information and sources and methods while maintaining its availability.

Feedback when correct:

That's right! You selected the correct responses.

The correct answers are:

PERSEC - Assesses the loyalty reliability, and trustworthiness of individuals holding or requesting a clearance.

Physical and Technical Security - Prevents unauthorized access to, and detects attempts at, unauthorized access to physical or communication technologies.

Information Assurance and Cyber Security - Develops and implements policies and procedures for IT systems security risk management, certification, and accreditation.

Classification Management - Provides the IC procedures for protecting intelligence information and sources and methods while maintaining its availability.

Feedback when incorrect:

You did not select the correct responses.

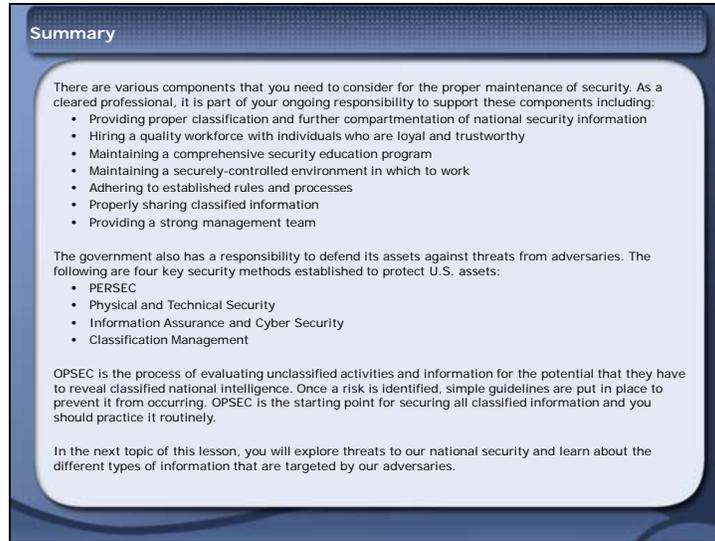
The correct answers are:

PERSEC - Assesses the loyalty reliability, and trustworthiness of individuals holding or requesting a clearance.

Physical and Technical Security - Prevents unauthorized access to, and detects attempts at, unauthorized access to physical or communication technologies.

Information Assurance and Cyber Security - Develops and implements policies and procedures for IT systems security risk management, certification, and accreditation.

Classification Management - Provides the IC procedures for protecting intelligence information and sources and methods while maintaining its availability.



Summary

There are various components that you need to consider for the proper maintenance of security. As a cleared professional, it is part of your ongoing responsibility to support these components including:

- Providing proper classification and further compartmentation of national security information
- Hiring a quality workforce with individuals who are loyal and trustworthy
- Maintaining a comprehensive security education program
- Maintaining a securely-controlled environment in which to work
- Adhering to established rules and processes
- Properly sharing classified information
- Providing a strong management team

The government also has a responsibility to defend its assets against threats from adversaries. The following are four key security methods established to protect U.S. assets:

- PERSEC
- Physical and Technical Security
- Information Assurance and Cyber Security
- Classification Management

OPSEC is the process of evaluating unclassified activities and information for the potential that they have to reveal classified national intelligence. Once a risk is identified, simple guidelines are put in place to prevent it from occurring. OPSEC is the starting point for securing all classified information and you should practice it routinely.

In the next topic of this lesson, you will explore threats to our national security and learn about the different types of information that are targeted by our adversaries.

Summary

There are various components that you need to consider for the proper maintenance of security. As a cleared professional, it is part of your ongoing responsibility to support these components including:

- Providing proper classification and further compartmentation of national security information
- Hiring a quality workforce with individuals who are loyal and trustworthy
- Maintaining a comprehensive security education program
- Maintaining a securely-controlled environment in which to work
- Adhering to established rules and processes
- Properly sharing classified information
- Providing a strong management team

The government also has a responsibility to defend its assets against threats from adversaries. The following are four key security methods established to protect U.S. assets:

- PERSEC
- Physical and Technical Security
- Information Assurance and Cyber Security
- Classification Management

OPSEC is the process of evaluating unclassified activities and information for the potential that they have to reveal classified national intelligence. Once a risk is identified, simple guidelines are put in place to prevent it from occurring. OPSEC is the starting point for securing all classified information and you should practice it routinely.

In the next topic of this lesson, you will explore threats to our national security and learn about the different types of information that are targeted by our adversaries.



Lesson 1: Welcome to Security in the IC Introduction

Topic 1.4: Threats to National Security

Introduction and Objectives

Determining who, or what, is a threat to national security is not an easy task. Sometimes we realize a threat only after we have been compromised or subjected to a catastrophic event (e.g., Pearl Harbor, September 11). Other times, we are able to predict new threats by assessing and analyzing the political, environmental, and/or economic climate of other nations.

Security processes are put into place to protect us against persistent and emerging threats. It is essential that you are aware of these threats and prevent disclosure of information to an unauthorized recipient.

Objectives

- Describe threats to security
- Identify the types of information our adversaries are trying to target
- Define espionage and describe how it is a threat to national security
- Identify the characteristics of someone who may be susceptible to espionage
- Identify what you should do if you suspect espionage

"The United States faces a complex and rapidly changing national security environment in which nation-states, highly capable non-state actors, and other transnational forces will continue to compete with and challenge U.S. national interests. Adversaries are likely to use asymmetric means and technology (either new or applied in a novel way) to counter U.S. interests at home and abroad."

-NIS, 2009

Introduction and Objectives

Determining who, or what, is a threat to national security is not an easy task. Sometimes we realize a threat only after we have been compromised or subjected to a catastrophic event (e.g., Pearl Harbor, September 11). Other times, we are able to predict new threats by assessing and analyzing the political, environmental, and/or economic climate of other nations.

Security processes are put into place to protect us against persistent and emerging threats. It is essential that you are aware of these threats and prevent disclosure of information to an unauthorized recipient.

Objectives

- Describe threats to security
- Identify the types of information our adversaries are trying to target
- Define espionage and describe how it is a threat to national security
- Identify the characteristics of someone who may be susceptible to espionage
- Identify what you should do if you suspect espionage

Call-Out Box: "The United States faces a complex and rapidly changing national security environment in which nation-states, highly capable non-state actors, and other transnational forces will continue to compete with and challenge U.S. national interests. Adversaries are likely to use asymmetric means and technology (either new or applied in a novel way) to counter U.S. interests at home and abroad."

-NIS, 2009



Threats to Security

Introduction

There are many internal and external threats to our national security. As a cleared professional, one of your responsibilities is to be aware of threats that might lead to potential security compromises.

Select the (+) by each term for more information on these common threats.

(Image Alt: Common security threats: moles, traitors, bad security habits, unauthorized disclosures, terrorists, foreign intelligence services, hackers, and activists)

Traitors

A traitor is a U.S. citizen or person who commits treason (spies for another nation state or group looking to damage U.S. interests) either voluntarily or by recruitment.

Foreign Intelligence Services

A Foreign Intelligence Service is a nation state's organization, agency, or service responsible for foreign operations, intelligence-gathering and analysis, and the exchange of intelligence information.

Moles

A mole is a person who infiltrates a job in one nation, but is actually spying for an adversarial nation state. Moles are also traitors. However, unlike some recruits or volunteers who were coerced into espionage, these people take a job requiring a security clearance with the intention of spying.

Terrorists

A terrorist is an individual who commits an act (or acts) of violence or threatens violence in pursuit of political, religious, or ideological objectives.

Activists

Activists can be individuals, a group or collection of people, or an organization that advocates, threatens, uses force or violence, or any other illegal or unconstitutional means in an effort to do one or more of the following things:

- Overthrow or influence the government (federal, state, local, or tribal)
- Prevent government personnel from performing their official duties
- Gain retribution for perceived wrongs caused by the government
- Prevent others from exercising their rights under the Constitution or federal and state laws

Many activist groups are legal, but a few groups or members may use unlawful means to protest or gain publicity for their cause.

Bad Security Habits

Bad security habits include:

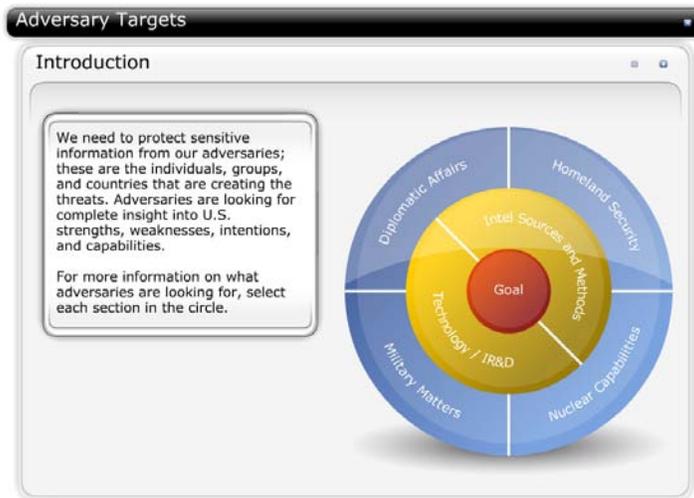
- "Talking around" classified information in a non-secure location, or alluding to the details of classified information without mentioning the specific subject
- "Piggy backing" or following another individual into a secure facility without badging-in
- Becoming complacent about security

Unauthorized Disclosures

An unauthorized disclosure is a communication or physical transfer of classified national intelligence information, including SCI, to an unauthorized recipient.

Hackers

A hacker is an individual who attempts to break into computer systems, write malware (i.e., viruses, spam, spyware, and other malicious software), and steal information.



Adversary Targets

Introduction

We need to protect sensitive information from our adversaries; these are the individuals, groups, and countries that are creating the threats. Adversaries are looking for complete insight into U.S. strengths, weaknesses, intentions, and capabilities.

For more information on what adversaries are looking for, select each section in the circle.

(Image Alt: Target with three levels labeled from the center out: Goal; Technology / IR&D, Intel Sources and Methods; Military Matters, Diplomatic Affairs, Homeland Security, Nuclear Capabilities)

Goal

SCI is what we know about our adversaries, how we collect the information, how successful we are at collecting it, and what our requirements and targets are. Our adversaries' goal is ultimately to destroy U.S. intelligence collection capabilities or use their knowledge of our capabilities to implement deception measures against us.

For this reason, classified security protection is about protecting information.

Technology / IR&D

Technology / Internal Research & Development (IR&D) includes information about:

- New technologies we are developing
- Potential applications of these new technologies

Intel Sources and Methods

Intelligence Sources and Methods includes information about how intelligence is collected. Sources and methods of intelligence collection take time to develop and can be compromised very quickly. SCI procedures were developed to protect this type of information.

Military Matters

Military Matters include information about:

- Our strengths and weakness
- Location of our troops
- Our equipment
- Our plans
- Our doctrine and tactics

Diplomatic Affairs

Diplomatic Affairs include information about:

- With whom we are talking
- Whom we are monitoring
- Countries we are sanctioning
- Our intentions

Homeland Security

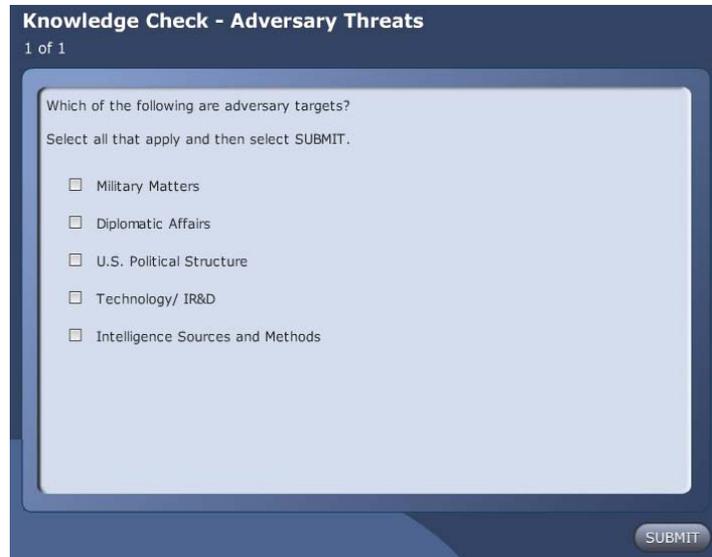
Homeland Security (Infrastructure) includes information about:

- Our critical infrastructure
- Our critical infrastructure vulnerabilities
- The impact to our society, our government, and the public's confidence in the government, if our critical infrastructure is compromised

Nuclear Capabilities

Nuclear Capabilities include information about:

- Our nuclear capabilities status
- Our knowledge of the nuclear capabilities of others
- Technologies surrounding nuclear capabilities



Knowledge Check - Adversary Threats

1. Which of the following are adversary targets?

Select all that apply and then select SUBMIT.

Choice
Military Matters
Diplomatic Affairs
U.S. Political Structure
Technology/ IR&D
Intelligence Sources and Methods

The following table reflects the correct answers.

Correct	Choice
X	Military Matters
X	Diplomatic Affairs
	U.S. Political Structure
X	Technology/ IR&D
X	Intelligence Sources and Methods

Feedback when correct:

That's right! You have selected the correct responses.

The following are adversary targets:

- Military Matters
- Diplomatic Affairs
- Technology/IR&D
- Intelligence Sources and Methods

U.S. Political Structure is public domain information and not an adversary target.

Feedback when incorrect:

You did not select the correct responses.

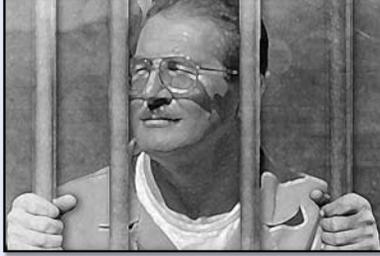
The following are adversary targets:

- Military Matters
- Diplomatic Affairs
- Technology/IR&D
- Intelligence Sources and Methods

U.S. Political Structure is public domain information and not an adversary target.

Espionage in the U.S.

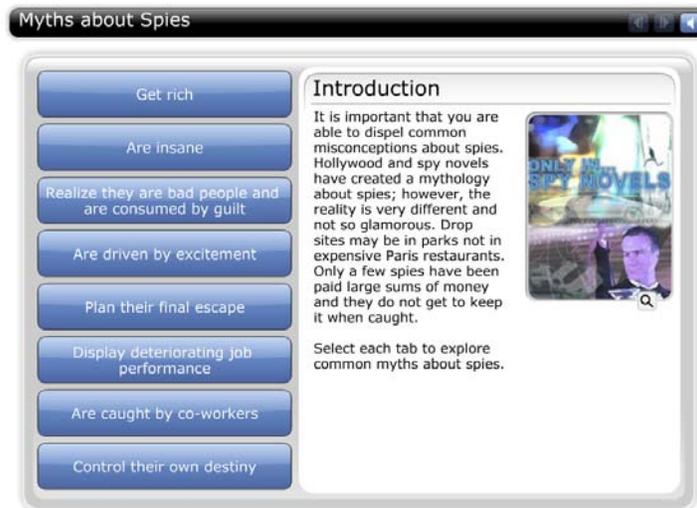
Espionage can be defined as stealing information that governments or organizations are trying to protect. One spy can cause significant damage to intelligence collection by divulging information about our intelligence sources and methods. For example, while Aldrich Ames worked for the CIA, he spied for the Soviet KGB in the 1980s. His betrayal resulted in significant damage to our national security and caused the deaths of numerous people (intelligence sources). Foreign connections will be explored in depth in Lesson 2.

A black and white photograph of Aldrich Ames, a former CIA spy, looking out from behind vertical metal bars. He is wearing glasses and a light-colored shirt. The image is framed within a blue-bordered box that also contains text.

Espionage in the U.S.

Espionage can be defined as stealing information that governments or organizations are trying to protect. One spy can cause significant damage to intelligence collection by divulging information about our intelligence sources and methods. For example, while Aldrich Ames worked for the CIA, he spied for the Soviet KGB in the 1980s. His betrayal resulted in significant damage to our national security and caused the deaths of numerous people (intelligence sources). Foreign connections will be explored in depth in Lesson 2.

(Image Alt: Aldrich Ames behind bars)



Myths about Spies

Introduction

It is important that you are able to dispel common misconceptions about spies. Hollywood and spy novels have created a mythology about spies; however, the reality is very different and not so glamorous. Drop sites may be in parks not in expensive Paris restaurants. Only a few spies have been paid large sums of money and they do not get to keep it when caught.

Select each tab to explore common myths about spies.

(Image Alt: Collage of concepts from spy movies and novels)

Get rich

Although most spies seem to be motivated by money, in reality they do not make much money and, if arrested, they must turn it over to the authorities.

Are insane

Spies are sometimes vulnerable because of their vices, but in general they are not mentally ill; most are perfectly cognizant of their actions.

Realize they are bad people and are consumed by guilt

Spies rationalize that their actions are "not that harmful" to national security or to people's safety.

Are driven by excitement

Some spies may be coerced into spying, but most are driven by greed, not excitement.

Plan their final escape

Some spies may try to flee capture, but most do not have an escape plan.

Display deteriorating job performance

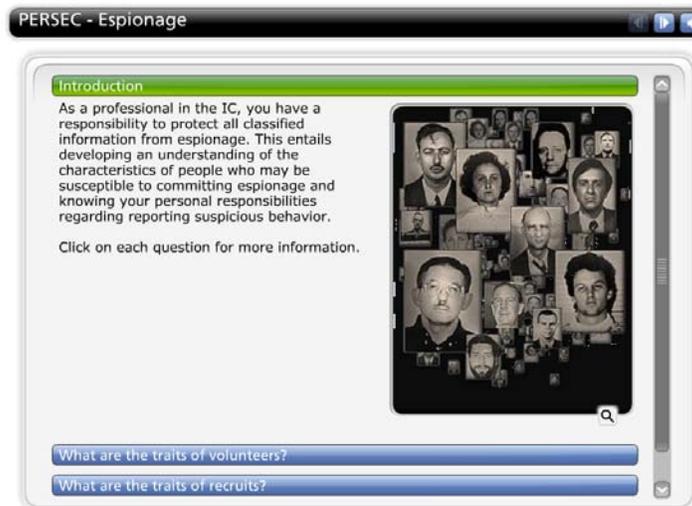
Spies do not usually display deteriorating job performance because they fear losing their access to classified information. However, most will show some outwardly suspicious behavior.

Are caught by co-workers

Unfortunately, it is only after a co-worker is arrested for espionage that people recall their co-worker's obviously suspicious behavior. Although co-workers can provide information to security on suspicious activity, many do not.

Control their own destiny

Spies are usually in a Catch-22 situation. Once they provide some information to their handler, they fear exposure to the authorities which motivates them to provide more and more information to their handler, which makes them even more vulnerable.



PERSEC - Espionage

Introduction

As a professional in the IC, you have a responsibility to protect all classified information from espionage. This entails developing an understanding of the characteristics of people who may be susceptible to committing espionage and knowing your personal responsibilities regarding reporting suspicious behavior.

Click on each question for more information.

(Image Alt: Collage of convicted spies)

What are the traits of volunteers?

In general, people who volunteer to commit espionage may exhibit some of the traits found in the following categories:

- Narcissism and grandiosity
 - Are narcissistic and show signs of grandiosity
 - Think of themselves as high achievers
 - Think they have special talents that are not recognized by supervisors
 - Rate themselves higher in their personal evaluations than their supervisors do
 - Like to be the center of attention
 - Ask for more favors than they deserve

- Distorted sense of entitlement
 - Have a distorted sense of entitlement and may be immature and naive in the ways of the world
 - Anticipate promotions that are not coming
 - Are manipulative and self-serving
 - Crave immediate satisfaction

- Reactions to achievement and criticism
 - Display immaturity with regard to achievements
 - React negatively to criticism

- Relationships with others
 - Are envious of others
 - Have a hard time getting along with coworkers
 - Do not seek close personal relationships
 - Are insensitive to others; demonstrate prejudice
 - Take advantage of, or use, other people

- Antisocial behaviors
 - Exhibit antisocial behavior
 - Have a lack of attachment or commitment

- Rationalize criminal behavior
 - Are able to rationalize criminal behavior - believe that they are not really betraying their country
 - Have a lack of guilt or remorse

- Compulsive behaviors
 - Drink excessively or use drugs
 - Spend money they don't have

- Regard for rules and obligations
 - Press the limits of rules
 - Disregard security rules
 - Ignore or neglect obligations
 - Are frequently tardy or leave early for no good reason

What are the traits of recruits?

In general, people who are recruited to commit espionage may exhibit some of the traits found in the following categories:

- Esteem
 - Lack self esteem
 - Are easily swayed by others
 - Are uncomfortable in strange surroundings
 - Are uncomfortable with sexual identity

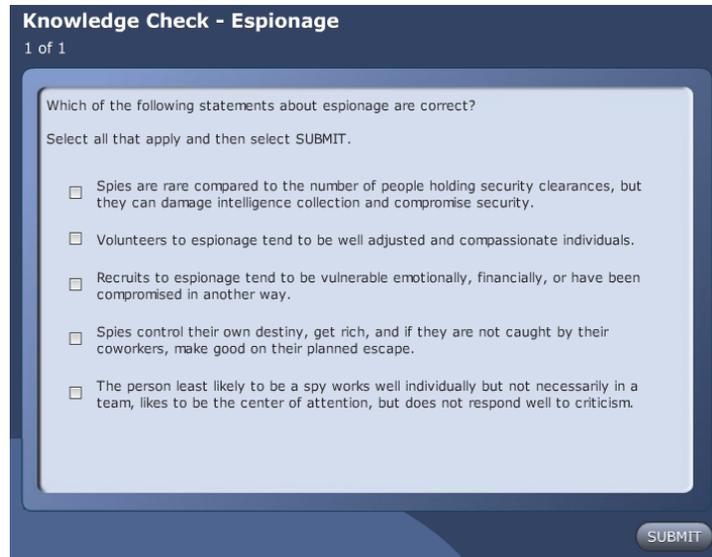
- Professional Relationships
 - Are not good team players
 - Are good individual contributors
 - Have a hard time getting along with coworkers

- Personal Relationships
 - Have unstable (or no) relationships
 - Do not seek close personal relationships
 - Never seem warm or sympathetic
 - Are insensitive to others; demonstrate prejudice
 - Take advantage of, or use, other people

What do I do if I think someone is a spy?

Finding or unmasking espionage is largely a counterintelligence responsibility. However, the potential damage to national security makes it imperative that you follow up on your suspicions using the appropriate channels. Be observant of other cleared personnel, and if you become suspicious of someone's behavior or suspect someone may be involved in espionage do the following:

- Report individuals who demonstrate deviant behavioral traits.
- Immediately report your suspicions **only** to your Special Security Officer (SSO) and/or manager



Knowledge Check - Espionage

1. Which of the following statements about espionage are correct?

Select all that apply and then select SUBMIT.

Choice
Spies are rare compared to the number of people holding security clearances, but they can damage intelligence collection and compromise security.
Volunteers to espionage tend to be well adjusted and compassionate individuals.
Recruits to espionage tend to be vulnerable emotionally, financially, or have been compromised in another way.
Spies control their own destiny, get rich, and if they are not caught by their coworkers, make good on their planned escape.
The person least likely to be a spy works well individually but not necessarily in a team, likes to be the center of attention, but does not respond well to criticism.

The following table reflects the correct answers.

Correct	Choice
X	Spies are rare compared to the number of people holding security clearances, but they can damage intelligence collection and compromise security.
	Volunteers to espionage tend to be well adjusted and compassionate individuals.
X	Recruits to espionage tend to be vulnerable emotionally, financially, or have been compromised in another way.
	Spies control their own destiny, get rich, and if they are not caught by their coworkers, make good on their planned escape.
	The person least likely to be a spy works well individually but not necessarily in a team, likes to be the center of attention, but does not respond well to criticism.

Feedback when correct:

That's right! You have selected the correct responses.

The following statements about espionage are correct:

- Spies are rare compared to the number of people holding security clearances, but they can damage intelligence collection and compromise security
- Recruits to espionage tend to be vulnerable emotionally, financially, or have been compromised in another way

The other options are incorrect because:

- Volunteers to espionage **do not** tend to be well adjusted or compassionate individuals
- Spies often **do not** control their own destiny, generally **do not** make much money, are **rarely** caught by their coworkers, and most **have never** planned an escape
- Common traits of people who volunteer for espionage **include** a tendency to work well individually but not necessarily in a team, and the desire to be the center of attention but to not respond well to criticism

Feedback when incorrect:

You did not select the correct responses.

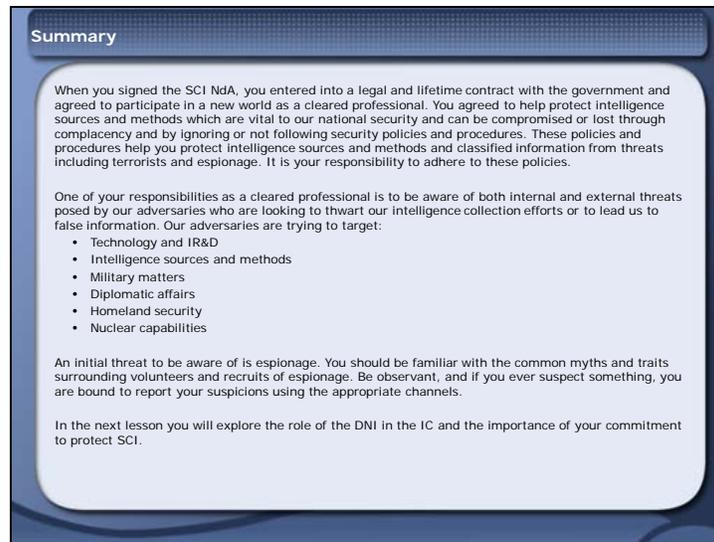
The following statements about espionage are correct:

- Spies are rare compared to the number of people holding security clearances, but they can damage intelligence collection and compromise security
- Recruits to espionage tend to be vulnerable emotionally, financially, or have been compromised in another way

The other options are incorrect because:

- Volunteers to espionage **do not** tend to be well adjusted or compassionate individuals
- Spies often **do not** control their own destiny, generally **do not** make much money, are **rarely** caught by their coworkers, and most **have never** planned an escape

- Common traits of people who volunteer for espionage **include** a tendency to work well individually but not necessarily in a team, and the desire to be the center of attention but to not respond well to criticism



Summary

When you signed the SCI NDA, you entered into a legal and lifetime contract with the government and agreed to participate in a new world as a cleared professional. You agreed to help protect intelligence sources and methods which are vital to our national security and can be compromised or lost through complacency and by ignoring or not following security policies and procedures. These policies and procedures help you protect intelligence sources and methods and classified information from threats including terrorists and espionage. It is your responsibility to adhere to these policies.

One of your responsibilities as a cleared professional is to be aware of both internal and external threats posed by our adversaries who are looking to thwart our intelligence collection efforts or to lead us to false information. Our adversaries are trying to target:

- Technology and IR&D
- Intelligence sources and methods
- Military matters
- Diplomatic affairs
- Homeland security
- Nuclear capabilities

An initial threat to be aware of is espionage. You should be familiar with the common myths and traits surrounding volunteers and recruits of espionage. Be observant, and if you ever suspect something, you are bound to report your suspicions using the appropriate channels.

In the next lesson you will explore the role of the DNI in the IC and the importance of your commitment to protect SCI.

Summary

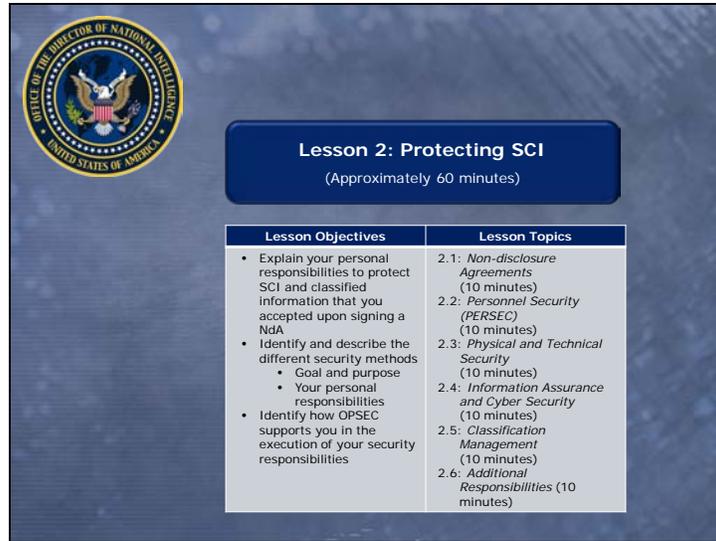
When you signed the SCI NDA, you entered into a legal and lifetime contract with the government and agreed to participate in a new world as a cleared professional. You agreed to help protect intelligence sources and methods which are vital to our national security and can be compromised or lost through complacency and by ignoring or not following security policies and procedures. These policies and procedures help you protect intelligence sources and methods and classified information from threats including terrorists and espionage. It is your responsibility to adhere to these policies.

One of your responsibilities as a cleared professional is to be aware of both internal and external threats posed by our adversaries who are looking to thwart our intelligence collection efforts or to lead us to false information. Our adversaries are trying to target:

- Technology and IR&D
- Intelligence sources and methods
- Military matters
- Diplomatic affairs
- Homeland security
- Nuclear capabilities

An initial threat to be aware of is espionage. You should be familiar with the common myths and traits surrounding volunteers and recruits of espionage. Be observant, and if you ever suspect something, you are bound to report your suspicions using the appropriate channels.

In the next lesson you will explore the role of the DNI in the IC and the importance of your commitment to protect SCI.

The slide features the Office of the Director of National Intelligence logo in the top left corner. The main title is "Lesson 2: Protecting SCI" with a subtitle "(Approximately 60 minutes)". Below this is a table with two columns: "Lesson Objectives" and "Lesson Topics".

Lesson Objectives	Lesson Topics
<ul style="list-style-type: none">• Explain your personal responsibilities to protect SCI and classified information that you accepted upon signing a Nda• Identify and describe the different security methods<ul style="list-style-type: none">• Goal and purpose• Your personal responsibilities• Identify how OPSEC supports you in the execution of your security responsibilities	<ul style="list-style-type: none">2.1: <i>Non-disclosure Agreements</i> (10 minutes)2.2: <i>Personnel Security (PERSEC)</i> (10 minutes)2.3: <i>Physical and Technical Security</i> (10 minutes)2.4: <i>Information Assurance and Cyber Security</i> (10 minutes)2.5: <i>Classification Management</i> (10 minutes)2.6: <i>Additional Responsibilities</i> (10 minutes)

Lesson 2: Protecting SCI

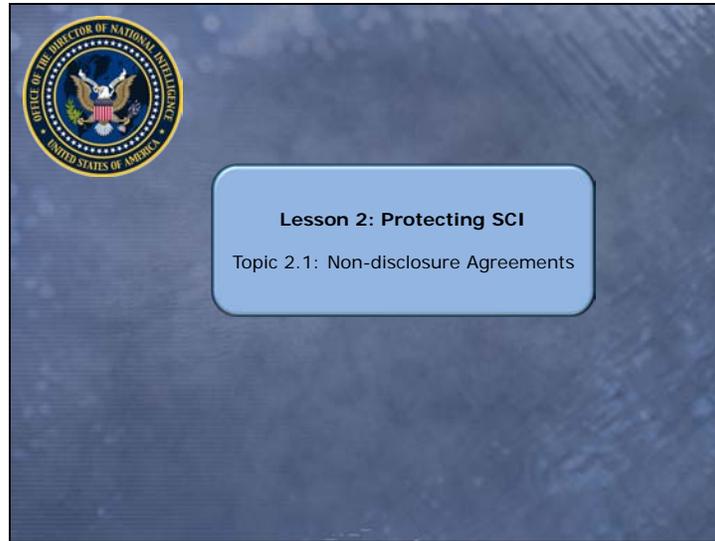
(Approximately 60 minutes)

Lesson Objectives

- Explain your personal responsibilities to protect SCI and classified information that you accepted upon signing a Nda
- Identify and describe the different security methods
 - Goal and purpose
 - Your personal responsibilities
- Identify how OPSEC supports you in the execution of your security responsibilities

Lesson Topics

- 2.1: *Non-disclosure Agreements* (10 minutes)
- 2.2: *Personnel Security (PERSEC)* (10 minutes)
- 2.3: *Physical and Technical Security* (10 minutes)
- 2.4: *Information Assurance and Cyber Security* (10 minutes)
- 2.5: *Classification Management* (10 minutes)
- 2.6: *Additional Responsibilities* (10 minutes)



Lesson 2: Protecting SCI

Topic 2.1: Non-disclosure Agreements

Introduction and Objectives

In Lesson 1, you learned about the makeup of the IC, how information is classified, and threats to our national security and national intelligence information. Some of this information is placed into formal SCI Control Systems. Only individuals who have been granted formal access by the information manager to compartments in that control system are allowed to view that information.

As a cleared professional, the U.S. Government has entrusted you with the protection of that information by granting you a security clearance and SCI eligibility. When you were given your initial security briefing, you signed an SCI Nda, a contract between you and the U.S. Government.

This topic covers the purpose, make up, and legal basis for the SCI Nda, and your personal responsibilities as an SCI professional.

Objectives

- Define the purpose of the SCI Nda
- Describe the legal basis and governing documents supporting the Nda
- Explain the elements of the Nda
- Identify your personal responsibility as an SCI-approved professional



Introduction and Objectives

In Lesson 1, you learned about the makeup of the IC, how information is classified, and threats to our national security and national intelligence information. Some of this information is placed into formal SCI Control Systems. Only individuals who have been granted formal access by the information manager to compartments in that control system are allowed to view that information.

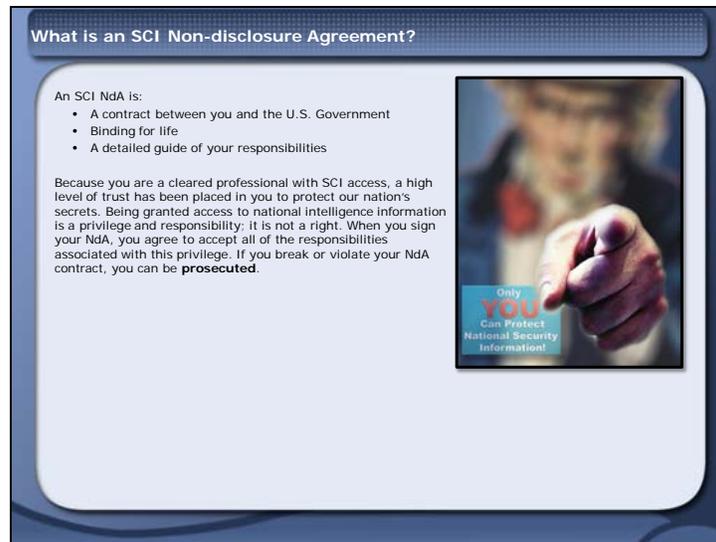
As a cleared professional, the U.S. Government has entrusted you with the protection of that information by granting you a security clearance and SCI eligibility. When you were given your initial security briefing, you signed an SCI Nda, a contract between you and the U.S. Government.

This topic covers the purpose, make up, and legal basis for the SCI Nda, and your personal responsibilities as an SCI professional.

Objectives

- Define the purpose of the SCI Nda
- Describe the legal basis and governing documents supporting the Nda
- Explain the elements of the Nda
- Identify your personal responsibility as an SCI-approved professional

(Image Alt: Collage of hands shaking, the Capitol, legal documents, eye glasses, and a pen)



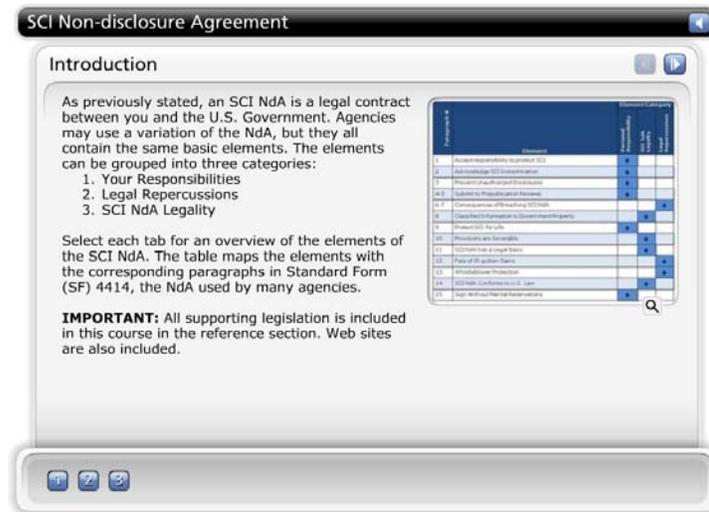
What is an SCI Non-disclosure Agreement?

An SCI NdA is:

- A contract between you and the U.S. Government
- Binding for life
- A detailed guide of your responsibilities

Because you are a cleared professional with SCI access, a high level of trust has been placed in you to protect our nation's secrets. Being granted access to national intelligence information is a privilege and responsibility; it is not a right. When you sign your NdA, you agree to accept all of the responsibilities associated with this privilege. If you break or violate your NdA contract, you can be **prosecuted**.

(Image Alt: Uncle Sam pointing; sign reading, "Only You Can Protect National Security Information!")



SCI Non-disclosure Agreement

Introduction

As previously stated, an SCI NdA is a legal contract between you and the U.S. Government. Agencies may use a variation of the NdA, but they all contain the same basic elements. The elements can be grouped into three categories:

1. Your Responsibilities
2. Legal Repercussions
3. SCI NdA Legality

Select each tab for an overview of the elements of the SCI NdA. The table maps the elements with the corresponding paragraphs in Standard Form (SF) 4414, the NdA used by many agencies.

IMPORTANT: All supporting legislation is included in this course in the reference section. Web sites are also included.

(Image Alt: A chart listing the paragraph numbers for the Elements of an NdA and the Categories under which they fall)

Your Responsibilities

By signing the NdA, you agree to the following responsibilities:

1. **You accept the responsibility to protect SCI.**
2. **You acknowledge your indoctrination.** This includes being briefed on your security responsibilities, having access to SCI, and your awareness of SCI programs.
3. **You agree to prevent unauthorized disclosures.** An unauthorized disclosure is a communication or physical transfer of classified national intelligence, including SCI, to an unauthorized recipient. To prevent unauthorized disclosures, you must verify that the intended recipient of SCI information is a cleared professional with the appropriate SCI access.

- 4. You agree to submit to a pre-publication review.** A pre-publication review is needed for any information that you intend to place into the public domain for non-official reasons which is based upon knowledge that you have gained from SCI access.
- 5. You agree to protect SCI for life.** By signing the SCI NDA contract you are making a lifelong commitment to protect U.S. Government classified intelligence information. Even if you are debriefed or no longer hold a clearance, you are responsible for protecting classified information.
- 6. You understand and agree to the terms of the contract without any mental reservations.**

Legal Repercussions

By signing the NDA, you are acknowledging that you understand the following legal repercussions:

- 1. Breach of contract.** The consequences include, but are not limited to:
 - Loss of your clearance
 - Loss of your job
 - Imprisonment
 - Fines
- 2. The fate of ill-gotten gains.** If you profit from illegally disclosing classified information, that money will be surrendered to the Federal Government.
- 3. The whistleblower protections.** Signing the SCI NDA does not remove your whistleblower protections. However, you are still responsible for protecting classified information. Make sure that you only provide it to someone authorized to receive it, for example, your SSO or government point of contact.

SCI NDA Legality

By signing the NDA, you are acknowledging that you understand the following SCI NDA legalities:

- 1. Classified information is the property of the U.S. Government.** If information is classified, it is U.S. Government property. In fact, an OCA can only classify information that belongs to, and is under the control of, the U.S. Government.
- 2. The provisions of the NDA are severable.** If any part of the SCI NDA is ruled as illegal or unconstitutional, that section is severable from the rest of the agreement. However, the remainder of the SCI NDA is still binding and in effect.
- 3. The legal basis for the NDA.** This comes from sections 793, 794, 798, and 952 of *Title 18, U.S. Code (USC)*, and Section 783(b) of *Title 50 USC*, and *EO 13526*.
- 4. The SCI NDA conforms to U.S. law.**

Governing Documents

Remember, the SCI NdA is a legally binding contract between you and the U.S. Government. It is based on an EO and several laws, and is supported by the following governing documents:

- *EO 13526, Part 4.1. (a)(2)*
- *32 CFR, Part 2001, subpart H Section 2001.80*
- *Title 18, USC, Sections 641, 793, 794, 798, 952*
- *Title 50, USC, Sections 421, 783(b)*
- *Title 5, USC, Sections 2302, 7211*
- *Title 10, USC, Section 1034*

NOTE: The SCI NdA has withstood numerous legal challenges, including some at the Supreme Court level.



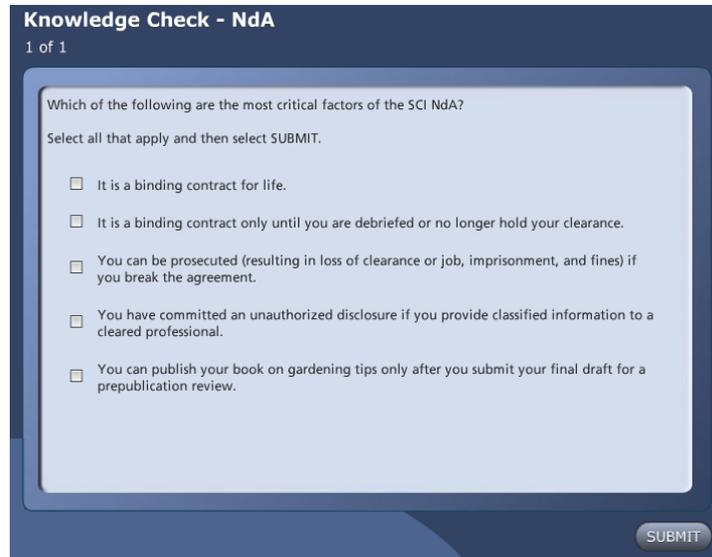
Governing Documents

Remember, the SCI NdA is a legally binding contract between you and the U.S. Government. It is based on an EO and several laws, and is supported by the following governing documents:

- EO 13526, Part 4.1. (a)(2)
- 32 CFR, Part 2001, subpart H Section 2001.80
- Title 18, USC, Sections 641, 793, 794, 798, 952
- Title 50, USC, Sections 421, 783(b)
- Title 5, USC, Sections 2302, 7211
- Title 10, USC, Section 1034

NOTE: The SCI NdA has withstood numerous legal challenges, including some at the Supreme Court level.

(Image Alt: Collage of legal documents, eye glasses, and a pen)



Knowledge Check - NdA

1. Which of the following are the most critical factors of the SCI NdA?

Select all that apply and then select SUBMIT.

Choice
It is a binding contract for life.
It is a binding contract only until you are debriefed or no longer hold your clearance.
You can be prosecuted (resulting in loss of clearance or job, imprisonment, and fines) if you break the agreement.
You have committed an unauthorized disclosure if you provide classified information to a cleared professional.
You can publish your book on gardening tips only after you submit your final draft for a prepublication review.

The following table reflects the correct answers.

Correct	Choice
X	It is a binding contract for life.
	It is a binding contract only until you are debriefed or no longer hold your clearance.
X	You can be prosecuted (resulting in loss of clearance or job, imprisonment, and fines) if you break the agreement.
	You have committed an unauthorized disclosure if you provide classified information to a cleared professional.
	You can publish your book on gardening tips only after you submit your final draft for a prepublication review.

Feedback when correct:

That's right! You have selected the correct responses.

- It is a binding contract for life
- You can be prosecuted (resulting in loss of clearance or job, imprisonment, and fines) if you break the agreement

The other answers are incorrect because:

- You are required to protect classified information even after you are debriefed or no longer hold a clearance
- You commit an unauthorized disclosure when you provide classified information to an **unauthorized** person
- You only need a prepublication review if the information you intend to publish is based on your classified experience

Feedback when incorrect:

You did not select the correct response.

The correct answers are:

- It is a binding contract for life
- You can be prosecuted (resulting in loss of clearance or job, imprisonment, and fines) if you break the agreement

The other answers are incorrect because:

- You are required to protect classified information even after you are debriefed or no longer hold a clearance
- You commit an unauthorized disclosure when you provide classified information to an **unauthorized** person
- You only need a prepublication review if the information you intend to publish is based on your classified experience



SCI Security Policy Development

Security requirements are written at the highest levels of government and are created to protect national secrets. The ODNI creates the implementation policies for the IC that provide consistent security protection methodologies for those who handle SCI. It is important that you understand and follow these policies.

National security orders and directives describe security policies, processes, and procedures. They are developed by the NSC and are issued in the name of the President of the U.S. in the form of EOs and Presidential Policy Directives (PPD). SCI protection policies, issued as ICDs in the name of the DNI, are an interpretation of these orders and directives.

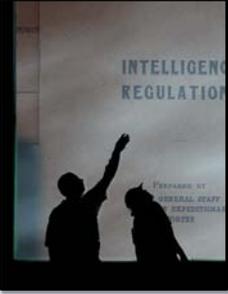
(Image Alt: Flow chart depicting the process followed to develop IC security policy and procedures)

Summary

Signing a Nda and accepting the responsibilities of working with sensitive information may be daunting. Guidelines to follow include:

- Understand your security responsibilities
- Exercise discipline in implementing your security responsibilities
- Work closely with security officers and keep them advised
- Release classified information only to a cleared professional with the appropriate SCI access and a need-to-know
- Only store, discuss, and process all classified information, to include SCI, within an SCI-accredited facility or Sensitive Compartmented Information Facility (SCIF)
- Never leave any classified information, to include SCI, unattended
- Never take classified information home
- Obtain security approval for all information system changes
- Be alert to threats and vulnerabilities and report them

In the next topic you will learn about PERSEC and your direct responsibilities as a cleared professional.



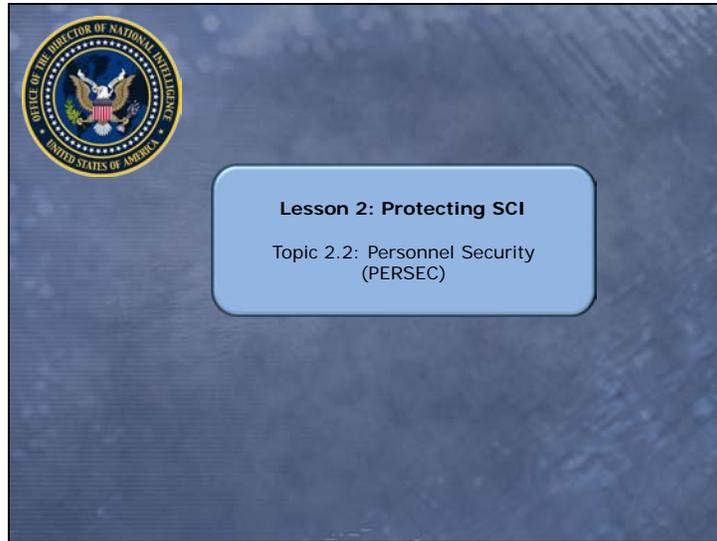
Summary

Signing a Nda and accepting the responsibilities of working with sensitive information may be daunting. Guidelines to follow include:

- Understand your security responsibilities
- Exercise discipline in implementing your security responsibilities
- Work closely with security officers and keep them advised
- Release classified information only to a cleared professional with the appropriate SCI access and a need-to-know
- Only store, discuss, and process all classified information, to include SCI, within an SCI-accredited facility or Sensitive Compartmented Information Facility (SCIF)
- Never leave any classified information, to include SCI, unattended
- Never take classified information home
- Obtain security approval for all information system changes
- Be alert to threats and vulnerabilities and report them

In the next topic you will learn about PERSEC and your direct responsibilities as a cleared professional.

(Image Alt: People reaching up to touch an Intelligence Regulation document)



Lesson 2: Protecting SCI

Topic 2.2: Personnel Security (PERSEC)

Introduction and Objectives

PERSEC assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information.

In this topic, you will learn the importance of properly reporting a variety of activities in order to maintain your clearance. These activities include personal activities, foreign travel, legal involvements, outside activities, and contact with the media.

Objectives

- Define and identify the purpose and goals of PERSEC
- Explain your responsibilities for PERSEC
- Describe the relationship between the characteristics of those who have committed espionage and personnel reporting requirements

REMEMBER!
PERSEC measures, such as assessing SCI eligibility, deter espionage and terrorism by ensuring that only reliable and trustworthy people are granted access to SCI.

Personnel Security

Introduction and Objectives

PERSEC assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information.

In this topic, you will learn the importance of properly reporting a variety of activities in order to maintain your clearance. These activities include personal activities, foreign travel, legal involvements, outside activities, and contact with the media.

Objectives

- Define and identify the purpose and goals of PERSEC
- Explain your responsibilities for PERSEC
- Describe the relationship between the characteristics of those who have committed espionage and personnel reporting requirements

REMEMBER!

PERSEC measures, such as assessing SCI eligibility, deter espionage and terrorism by ensuring that only reliable and trustworthy people are granted access to SCI.

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification management surrounded by Operations Security; Personnel Security is emphasized)

Reporting Activities

When you completed your security clearance application (*SF-86, Questionnaire for National Security Positions*), you documented a great deal of information concerning your personal life. This information was used to determine whether or not you could be trusted to work and protect national intelligence information.

As a cleared professional, you are one of our government's assets. You have:

- The necessary knowledge and skills
- Been entrusted with government secrets
- Made it through a lengthy and expensive clearance process

To maintain your clearance, you must report the following occurrences:

- Personal changes and concerns
- Foreign travel
- Foreign contacts

PERSEC reporting requirements can be found in *DCID 6/1* and *EO 13526*. Check with your SSO for additional guidance.

Let us explore each of these reportable activities.



Reporting Activities

When you completed your security clearance application (*SF-86, Questionnaire for National Security Positions*), you documented a great deal of information concerning your personal life. This information was used to determine whether or not you could be trusted to work and protect national intelligence information.

As a cleared professional, you are one of our government's assets. You have:

- The necessary knowledge and skills
- Been entrusted with government secrets
- Made it through a lengthy and expensive clearance process

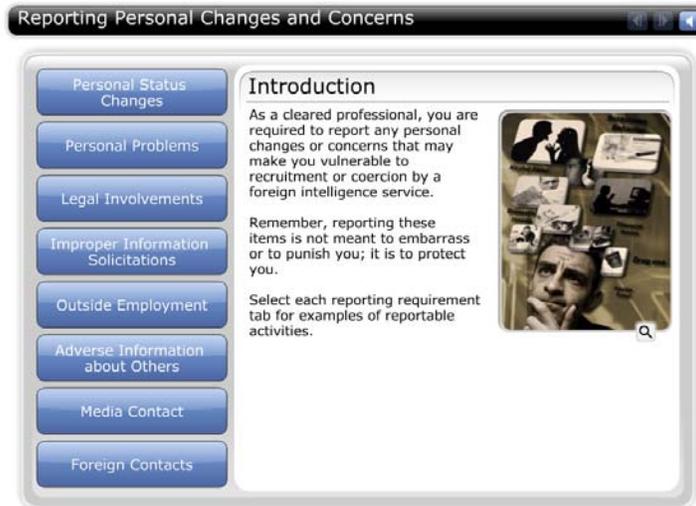
To maintain your clearance, you must report the following occurrences:

- Personal changes and concerns
- Foreign travel
- Foreign contacts

PERSEC reporting requirements can be found in *DCID 6/1* and *EO 13526*. Check with your SSO for additional guidance.

Let us explore each of these reportable activities.

(Image Alt: Collage of two people shaking hands at a conference, a passport, a man having a drink, and a globe)



Reporting Personal Changes and Concerns

Introduction

As a cleared professional, you are required to report any personal changes or concerns that may make you vulnerable to recruitment or coercion by a foreign intelligence service.

Remember, reporting these items is not meant to embarrass or to punish you; it is to protect you.

Select each reporting requirement tab for examples of reportable activities.

(Image Alt: Collage of a man puzzling over various personal issues)

Personal Status Changes

You must report any changes in your personal status including:

- Marriage
- Separation
- Divorce
- Cohabitation
- Adoption

Personal Problems

You must report any personal problems that you are dealing with such as:

- Financial issues
- Abuse or misuse of drugs (over-the-counter, prescription, and illicit)
- Abuse or misuse of alcohol (such as an arrest for Driving Under the Influence [DUI] of alcohol)

Legal Involvements

You must report any legal activities in which you are involved including:

- Litigation
- Arrest
- Court summons
- Jury duty

NOTE: Incidents such as parking tickets and minor traffic accidents do not need to be reported.

Improper Information Solicitations

You must report any improper solicitations for information that you receive. For example:

- Receiving requests for information about your work from unknown or unauthorized individuals
- Using improper protocols (bypassing security and export controls)

Outside Employment

You must report any outside employment. For example:

- Working at a store during the holiday season to earn extra money
- Volunteering to work for a political group in your city

Adverse Information about Others

You must report any adverse information about others that may affect your situation. For example, you would report a coworker experiencing any of the above situations without reporting them.

Media Contact

You must report any type of media contact that you have, whether initiated by you or the media. For example, a reporter receives your contact information from one of your friends and asks for your opinion on missile proliferation.

NOTE: You may be tempted to provide unclassified information on a project to a reporter. However, you should not have **any** media contact. You should always refer any requests from the media to your Public Affairs Office personnel who are authorized to interface with the media.

Foreign Contacts

You must report "a close and continuing relationship" with foreign persons. Examples include:

- Your in-laws are from France and are not U.S. citizens
- You are working with someone who is a Canadian citizen
- Your maid or nanny is from a foreign country
- Someone you chat with regularly on the Internet is from a foreign country

NOTE: Most foreign contacts are legitimate and well-meaning. Your ability to recognize the few who are not will help you to avoid problems. If you are not sure what information needs to be reported - talk to your SSO.

Reporting Foreign Travel

The world is a very diverse and interesting place, filled with a variety of people and travel destinations. Holding a security clearance does not keep you from meeting new people and traveling; however, it does require you to be cautious and to report these activities.

Your agency/organization will have a specific reporting process regarding foreign travel. Most trips must be reported in advance so that you can receive any required authorization and a pre-travel or defensive travel briefing. Depending on the security status of the country you plan to visit, a defensive travel briefing may be required because of your access to sensitive and classified information.

As a cleared professional in the IC, you need to report:

- All foreign travel in advance
- Any unusual trip incidents that make you feel uncomfortable. For example:
 - "Black market" activities
 - Changes in the itinerary
 - Requests for you to do something that appears to be illegal (e.g., exchanging money outside of an official means, transporting something into the country)

NOTE: Exceptions to the advance reporting rule are day trips to Mexico or Canada which can be reported upon your return.



BE AWARE!
A visit to a foreign embassy qualifies as foreign travel.

Reporting Foreign Travel

The world is a very diverse and interesting place, filled with a variety of people and travel destinations. Holding a security clearance does not keep you from meeting new people and traveling; however, it does require you to be cautious and to report these activities.

Your agency/organization will have a specific reporting process regarding foreign travel. Most trips must be reported in advance so that you can receive any required authorization and a pre-travel or defensive travel briefing. Depending on the security status of the country you plan to visit, a defensive travel briefing may be required because of your access to sensitive and classified information.

As a cleared professional in the IC, you need to report:

- All foreign travel in advance
- Any unusual trip incidents that make you feel uncomfortable. For example:
 - "Black market" activities
 - Changes in the itinerary
 - Requests for you to do something that appears to be illegal (e.g., exchanging money outside of an official means, transporting something into the country)

NOTE: Exceptions to the advance reporting rule are day trips to Mexico or Canada which can be reported upon your return.

BE AWARE!

A visit to a foreign embassy qualifies as foreign travel.

(Image Alt: Collage of Polaroid pictures of various foreign locations, a cruise ship, an embassy building, a Frenchman holding a baguette, a gondola, and a world map)

Reporting Foreign Contacts

It is not uncommon to come into contact with non-U.S. persons on a daily basis (e.g., professor, doctor, hairdresser, housekeeper, or colleague). The following information specifies when it is necessary to report a foreign contact.

Reportable Contact	Not Reportable Contact	Warning
<p>You have a close and continuing relationship (personal or professional) with a citizen, resident, or representative of a foreign country.</p> <p>NOTE: Contact via the Internet is also reportable, including:</p> <ul style="list-style-type: none">• Chat rooms• Email• Social networking sites	<p>You have casual contact with a citizen, resident, or representative of a foreign country, but not a close and continuing relationship.</p> <p>Non-reportable activities include:</p> <ul style="list-style-type: none">• Casual interactions with people in the service industry (e.g., hairdressers, contractors, plumbers)• Professional interactions with individuals at a conference• Social interactions at a party or gathering	<p>Casual conversations can become reportable.</p> <p>You must report a foreign contact if a citizen, resident, or representative of a foreign country solicits you for information, for example:</p> <ul style="list-style-type: none">• Shows a strong interest in your employment• Is not satisfied with your answers• Seeks follow-up contact

REMEMBER!
When in doubt, consult with your SSO.

Reporting Foreign Contacts

It is not uncommon to come into contact with non-U.S. persons on a daily basis (e.g., professor, doctor, hairdresser, housekeeper, or colleague). The following information specifies when it is necessary to report a foreign contact.

Reportable Contact

You have a **close** and **continuing** relationship (personal or professional) with a citizen, resident, or representative of a foreign country.

NOTE: Contact via the Internet is also reportable, including:

- Chat rooms
- Email
- Social networking sites

Not Reportable Contact

You have casual contact with a citizen, resident, or representative of a foreign country, but **not** a close and continuing relationship.

Non-reportable activities include:

- Casual interactions with people in the service industry (e.g., hairdressers, contractors, plumbers)
- Professional interactions with individuals at a conference
- Social interactions at a party or gathering

Warning

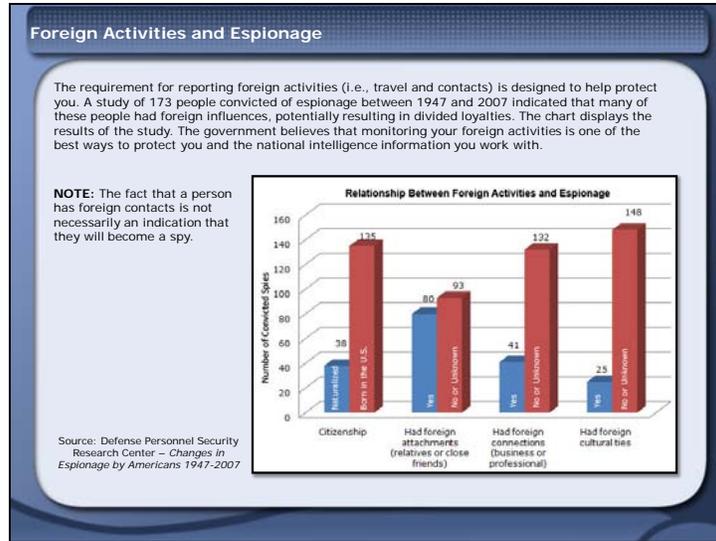
Casual conversations can become reportable.

You must report a foreign contact if a citizen, resident, or representative of a foreign country solicits you for information, for example:

- Shows a strong interest in your employment
- Is not satisfied with your answers
- Seeks follow-up contact

REMEMBER!

When in doubt, consult with your SSO.



Foreign Activities and Espionage

The requirement for reporting foreign activities (i.e., travel and contacts) is designed to help protect you. A study of 173 people convicted of espionage between 1947 and 2007 indicated that many of these people had foreign influences, potentially resulting in divided loyalties. The chart displays the results of the study. The government believes that monitoring your foreign activities is one of the best ways to protect you and the national intelligence information you work with.

NOTE: The fact that a person has foreign contacts is not necessarily an indication that they will become a spy.

Source: Defense Personnel Security Research Center – *Changes in Espionage by Americans 1947-2007*

(Image Alt: Chart labeled “Relationship Between Foreign Activities and Espionage”; provides the following data for convicted spies.

- Citizenship
 - Naturalized – 38
 - Born in the U.S. – 135
- Had foreign attachments (relatives or close friends)
 - Yes – 80
 - No or Unknown – 93
- Had foreign connections (business or professional)
 - Yes – 41
 - No or Unknown – 132
- Had foreign cultural ties
 - Yes – 25
 - No or Unknown – 148



Knowledge Check - Reportable Activities

1. As a person with a security clearance, you are required to report various personal activities.

Review the activities below. Select all that you would need to report and then select SUBMIT.

Choice
Attending a concert at the Austrian Embassy
Working in a study group with a non-U.S. citizen
Adopting a child
Reporting for jury duty
Bringing a cell phone into a SCIF
Presenting at a conference on missile proliferation
Getting a DUI
Getting a parking ticket
Missing a credit card payment
Keeping a blog about your personal life

The following table reflects the correct answers.

Correct	Choice
X	Attending a concert at the Austrian Embassy
X	Working in a study group with a non-U.S. citizen
X	Adopting a child
X	Reporting for jury duty
X	Bringing a cell phone into a SCIF
X	Presenting at a conference on missile proliferation
X	Getting a DUI
	Getting a parking ticket
	Missing a credit card payment
	Keeping a blog about your personal life

Feedback when correct:

That's right! You selected the correct responses.

The correct responses are:

- Attending a concert at the Austrian Embassy
- Working in a study group with a non-U.S. citizen
- Adopting a child
- Reporting for jury duty
- Bringing a cell phone into a SCIF
- Presenting at a conference on missile proliferation
- Getting a DUI

NOTE: Getting a parking ticket and missing a credit card payment are considered minor, non-reportable infractions. You may keep a blog, but you need to be mindful to not release professional information.

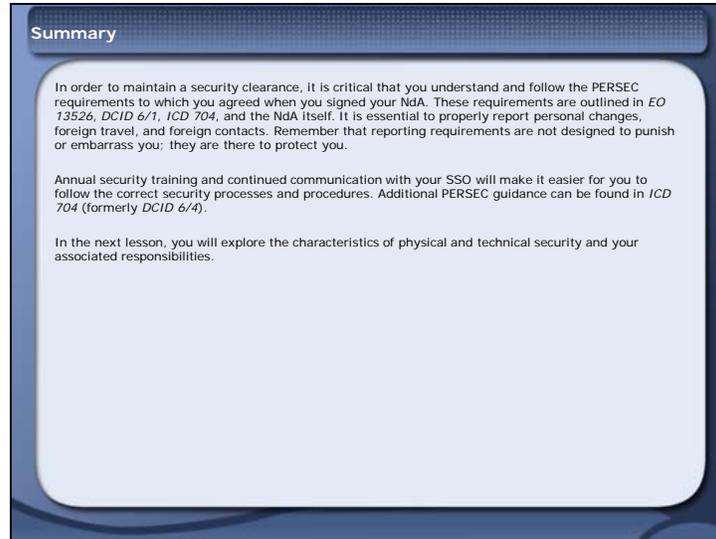
Feedback when incorrect:

You did not select the correct responses.

The correct responses are:

- Attending a concert at the Austrian Embassy
- Working in a study group with a non-U.S. citizen
- Adopting a child
- Reporting for jury duty
- Bringing a cell phone into a SCIF
- Presenting at a conference on missile proliferation
- Getting a DUI

NOTE: Getting a parking ticket and missing a credit card payment are considered minor, non-reportable infractions. You may keep a blog, but you need to be mindful to not release professional information.

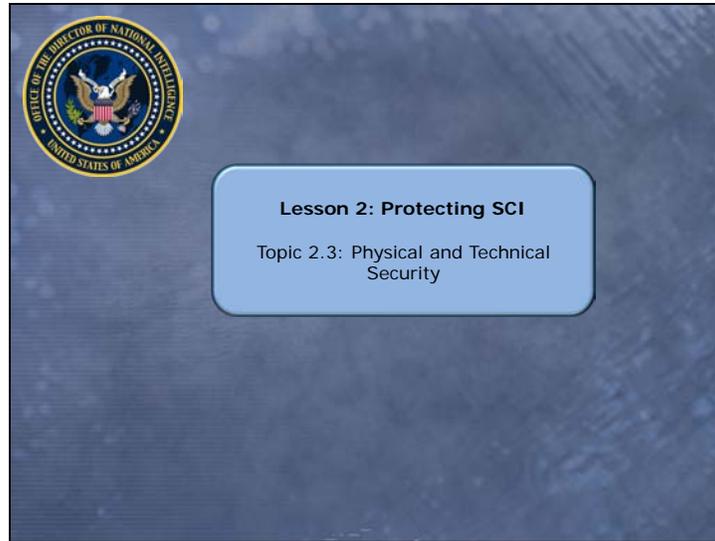


Summary

In order to maintain a security clearance, it is critical that you understand and follow the PERSEC requirements to which you agreed when you signed your NDA. These requirements are outlined in *EO 13526*, *DCID 6/1*, *ICD 704*, and the NDA itself. It is essential to properly report personal changes, foreign travel, and foreign contacts. Remember that reporting requirements are not designed to punish or embarrass you; they are there to protect you.

Annual security training and continued communication with your SSO will make it easier for you to follow the correct security processes and procedures. Additional PERSEC guidance can be found in *ICD 704* (formerly *DCID 6/4*).

In the next lesson, you will explore the characteristics of physical and technical security and your associated responsibilities.



Lesson 2: Protecting SCI

Topic 2.3: Physical and Technical Security

Introduction and Objectives

Physical and technical security methods are those that are the most visible – security measures such as formal access controls, locks, SCIFs, alarms, etc.

In this topic, you will explore various physical and technical security measures and practices that are in place to help protect national intelligence information, and the facilities in which it is processed, from compromise.

Objectives

- Define and identify the purpose and goals of physical and technical security
- Explain your responsibilities for physical and technical security
- Describe a SCIF
- Identify the purpose and characteristics of a SCIF
- Describe the protocols for working in a SCIF
- Identify operational security techniques you can apply within physical and technical security



Introduction and Objectives

Physical and technical security methods are those that are the most visible – security measures such as formal access controls, locks, SCIFs, alarms, etc.

In this topic, you will explore various physical and technical security measures and practices that are in place to help protect national intelligence information, and the facilities in which it is processed, from compromise.

Objectives

- Define and identify the purpose and goals of physical and technical security
- Explain your responsibilities for physical and technical security
- Describe a SCIF
- Identify the purpose and characteristics of a SCIF
- Describe the protocols for working in a SCIF
- Identify operational security techniques you can apply within physical and technical security

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification management surrounded by Operations Security; Physical & Technical Security is emphasized)

Purpose of Physical and Technical Security

Physical and technical security deals with the physical measures designed to:

- Protect personnel
- Prevent unauthorized access to facilities, equipment, materials, and documents
- Prevent the compromise of classified national intelligence information through communication technologies
- Prevent the compromise of classified national intelligence information through compromising emanations using TEMPEST, TSCM, and telecommunications security
- Defend against espionage, terrorism, sabotage, damage, and threat

Some of these physical and technical measures are built into the SCIF in which you work. One of the most important protective measures for classified information is ensuring that you know and practice good security behavior.

Physical and technical security guidance can be found in *ICD 705* (formerly *DCID 6/9*), *CNSS 7000*, *CNSS 500*, and *ICD 702*.



Purpose of Physical and Technical Security

Physical and technical security deals with the physical measures designed to:

- Protect personnel
- Prevent unauthorized access to facilities, equipment, materials, and documents
- Prevent the compromise of classified national intelligence information through communication technologies
- Prevent the compromise of classified national intelligence information through compromising emanations using TEMPEST, TSCM, and telecommunications security
- Defend against espionage, terrorism, sabotage, damage, and threat

Some of these physical and technical measures are built into the SCIF in which you work. One of the most important protective measures for classified information is ensuring that you know and practice good security behavior.

Physical and technical security guidance can be found in *ICD 705* (formerly *DCID 6/9*), *CNSS 7000*, *CNSS 500*, and *ICD 702*.

(Image Alt: Collage of barbed wire, a key pad lock, a camera phone, a security guard, a vault door, and a security camera)

What is a SCIF?

A SCIF is an area, installation, room, or group of rooms or buildings that is certified and accredited as meeting DNI security standards for the processing, storage, and discussion of SCI. Only SCI-approved persons may have unescorted access to a SCIF.

An unattended SCIF is always locked and alarmed. Some are guarded and staffed around the clock and do not close.

SCIFs must have the following physical and technical security elements:

- A solid entry door with a high-security lock and Access Control System
- A secure perimeter with walls that extend from true floor to true ceiling and provide sound protection
- An intrusion detection system
- Technical countermeasures (i.e., TEMPEST) to contain radio frequency emanations within a SCIF
- A telephone system that thwarts electronics eavesdropping

A photograph showing a person in silhouette walking away from a doorway. The doorway is brightly lit, and the person is walking into a darker area. The ceiling above the doorway has several circular lights or sensors.

What is a SCIF?

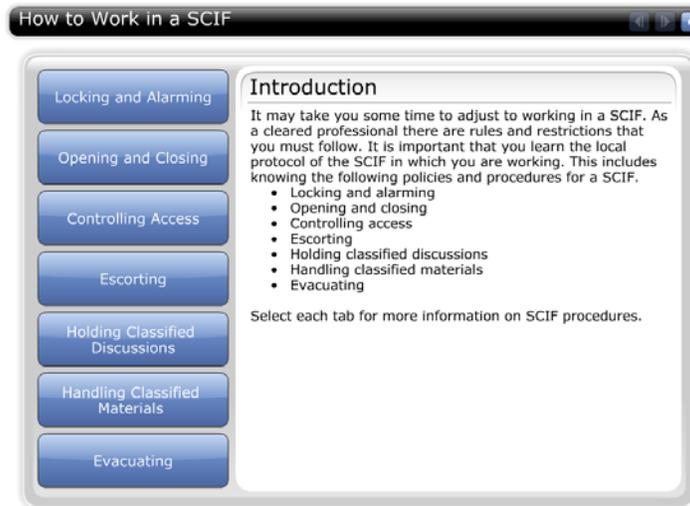
A SCIF is an area, installation, room, or group of rooms or buildings that is certified and accredited as meeting DNI security standards for the processing, storage, and discussion of SCI. Only SCI-approved persons may have unescorted access to a SCIF.

An unattended SCIF is always locked and alarmed. Some are guarded and staffed around the clock and do not close.

SCIFs must have the following physical and technical security elements:

- A solid entry door with a high-security lock and Access Control System
- A secure perimeter with walls that extend from true floor to true ceiling and provide sound protection
- An intrusion detection system
- Technical countermeasures (i.e., TEMPEST) to contain radio frequency emanations within a SCIF
- A telephone system that thwarts electronics eavesdropping

(Image Alt: A person exiting a SCIF)



How to Work in a SCIF

Introduction

It may take you some time to adjust to working in a SCIF. As a cleared professional there are rules and restrictions that you must follow. It is important that you learn the local protocol of the SCIF in which you are working. This includes knowing the following policies and procedures for a SCIF.

- Locking and alarming
- Opening and closing
- Controlling access
- Escorting
- Holding classified discussions
- Handling classified materials
- Evacuating

Select each tab for more information on SCIF procedures.

Locking and Alarming

When the SCIF is unattended, it needs to be locked and alarmed. If you are responsible for opening or closing the SCIF, you must:

- Learn the procedure for activating or deactivating the alarms
- Learn how to open and close the high-security lock

Practice these activities with your SSO. Learn what sets off the alarm (some alarms go off if too much time elapses between opening the high-security lock and turning off the alarm). You should know who to contact if the alarm sounds.

Opening and Closing

If you are responsible for opening or closing the SCIF, you need to know the procedures (such as the following) for that SCIF.

- Checking copiers and printers for classified information
- Ensuring safes are locked
- Walking through to ensure you are the last one there
- Locking the door and activating the alarm system

Controlling Access

Access to the SCIF should be carefully monitored by:

- Using a sign-in sheet
- Requiring all persons to wear a badge at all times when inside the SCIF
- Ensuring only SCI-approved persons have unescorted access to a SCIF
- Preventing an unauthorized/uncleared person from following you in to the SCIF (tailgating/piggybacking)

Escorting

Use the following tips when you escort an uncleared person in a SCIF:

- Have an adequate number of escorts
- Keep all uncleared persons in your visual control at all times
- Ensure that the escort is as technically competent as the uncleared person conducting work

Holding Classified Discussions

All SCI discussions stop at a SCIF door. Once you are outside of the SCIF, you are not in an appropriately-secured environment.

Handling Classified Materials

As a cleared professional, you will be responsible for the reproduction, destruction, storage, and transportation of classified materials. Classified information that is not safeguarded in an approved security container must be constantly under the control of a person having the proper security clearance and access. Because a SCIF is the only place where you are allowed to produce, process, store, or discuss classified information, you must know proper policies regarding classified materials. The table below reviews basic security policies for working with classified material.

Reproducing and Destroying

- Reproduce on approved equipment
- Use only approved destruction methods
 - Shredding
 - Burning
 - Pulping

Storing

- Store in an accredited facility and/or an approved container (e.g., SCIF, safe)

NOTE: Open storage is for material within an accredited SCIF that is not required to be stored in an approved Government Services Administration (GSA) container (i.e., safe). Closed storage is for classified material within an accredited SCIF that **must be** stored in an approved GSA container.

Transporting

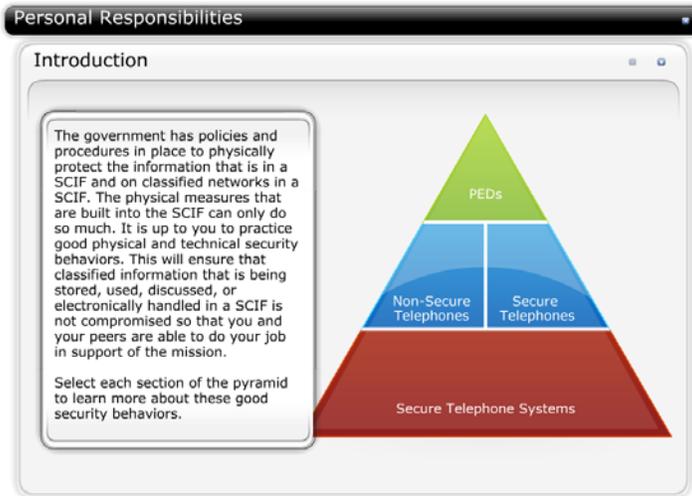
- Use of secure electronic systems to transmit classified information should always be the first choice, if at all possible
- Use receipts for all non-electronic transmissions (e.g., U.S. Postal Service)
- Use only approved devices (e.g., computers, networks, fax machines, etc.)
- Have materials carried by certified or designated couriers
- Wrap materials appropriately

Contact your SSO for local procedures and guidance.

Evacuating

Your security point of contact can tell you procedures that you need to follow in the event of an emergency, including:

- Securing classified information
- Evacuating the building
- Providing appropriate procedures to first responders



Personal Responsibilities

Introduction

The government has policies and procedures in place to physically protect the information that is in a SCIF and on classified networks in a SCIF. The physical measures that are built into the SCIF can only do so much. It is up to you to practice good physical and technical security behaviors. This will ensure that classified information that is being stored, used, discussed, or electronically handled in a SCIF is not compromised so that you and your peers are able to do your job in support of the mission.

Select each section of the pyramid to learn more about these good security behaviors.

(Image Alt: Pyramid with three levels: PEDs; Non-Secure Telephones, Secure Telephones; Secure Telephone Systems)

PEDs

Portable Electronic Devices (PED) are interesting and fun gadgets; however, they pose a risk to SCI if introduced into an SCI environment without proper authorization and review. The following are examples of PEDs:

- Personal Digital Assistants (PDA)
- Cellular phones
- MP3 players
- Cameras
- Flash drives
- Recordable media

These electronic devices can store, record, and/or transmit digital text, images, video, or audio. They may interact electrically or optically with other information systems in the SCIF.

You need to learn and follow the rules regarding the use of PEDs at your location. Contact your SSO for local procedures and guidance.

Non-Secure Telephones

Non-secure or "open" telephones are unclassified phones located inside the SCIF. You should practice the following behaviors while on an open telephone:

- Do not "talk around" classified information when using an open line
- Make sure that classified conversations are not taking place in the vicinity of an open telephone while it is in use
- Use the hold button when you step away from the instrument

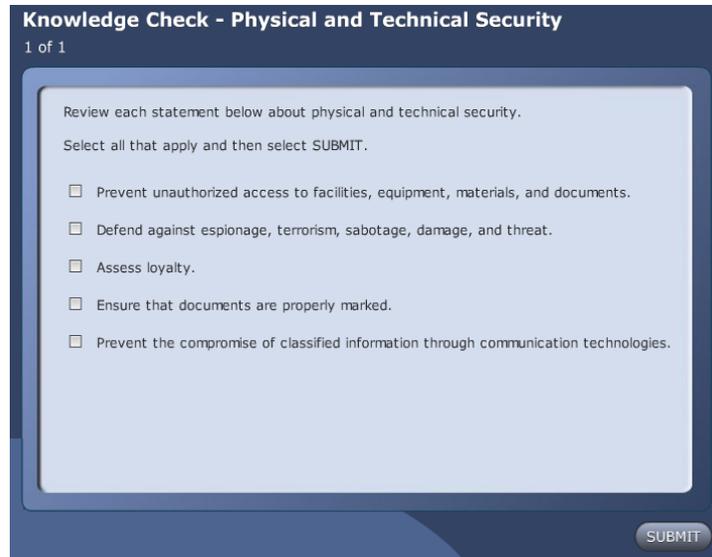
Secure Telephones

Secure telephones have been certified to handle classified conversations. Secure Telephone Equipment (STE) is any instrument that has been certified to handle classified information. The encryption takes place at the instrument and requires certain actions by the user for the phone to be in secure mode. Practice the following procedures:

- Use the appropriate keying device and/or press the secure button to ensure that your conversation is encrypted
- Check the LED on the phone to ensure it is in secure mode
- Check the classification level on the LED
- Reinitiate the secure mode if the encryption has been dropped - a tone on the phone may indicate this change
- Ensure that you "go secure" before you start any classified discussions
- Talk only at the established classification level indicated on the LED of the phone (i.e., do not "talk around" **TS/SCI** information if the phone is only encrypted at the **SECRET** level)

Secure Telephone Systems

Several agencies use secure telephone systems as well as STE. Using a secure telephone system does not require any action on your part; you pick up the phone and your conversation is encrypted. These secure telephones systems are bulk encrypted at the dedicated phone system.



Knowledge Check - Physical and Technical Security

1. Review each statement below about physical and technical security.

Select all that apply and then select SUBMIT.

Choice
Prevent unauthorized access to facilities, equipment, materials, and documents.
Defend against espionage, terrorism, sabotage, damage, and threat.
Assess loyalty.
Ensure that documents are properly marked.
Prevent the compromise of classified information through communication technologies.

The following table reflects the correct answers.

Correct	Choice
X	Prevent unauthorized access to facilities, equipment, materials, and documents.
X	Defend against espionage, terrorism, sabotage, damage, and threat.
	Assess loyalty.
	Ensure that documents are properly marked.
X	Prevent the compromise of classified information through communication technologies.

Feedback when correct:

That's right! You selected the correct responses.

Physical and technical security deals with the physical and technical measures designed to prevent unauthorized access to facilities, equipment, materials, and documents; to defend against espionage, terrorism, sabotage, damage, and threat; and prevent the compromise of classified information through communication technologies.

Assessing loyalty is a function of PERSEC and ensuring that documents are properly marked is a function of classification management.

Feedback when incorrect:

You did not select the correct responses.

Physical and technical security deals with the physical and technical measures designed to prevent unauthorized access to facilities, equipment, materials, and documents; prevent the compromise of classified information through communication technologies; and to defend against espionage, terrorism, sabotage, damage, and threat.

Assessing loyalty is a function of PERSEC and ensuring that documents are properly marked is a function of classification management.

Summary

Physical and technical security methods include measures such as formal access controls, locks, SCIFs, and alarms. These measures are put in place to protect personnel, facilities, equipment, materials, and documents. A SCIF is a specially designed location with physical and technical security elements that allow it to be certified and accredited by the DNI for the processing, storage, and discussion of SCI. As a cleared professional, it is critical that you understand the policies and procedures for a SCIF, including:

- Locking and alarming
- Opening and closing
- Controlling access
- Escorting
- Holding classified discussions
- Handling materials
- Evacuating

In addition, there are special rules for the proper use of phones and other telecommunication equipment of which you must be aware. Never take a phone, PED, or other two-way communication device into a SCIF.

In the next topic, you will discuss information assurance and cyber security. You will also learn your responsibilities and the government's responsibilities in relation to information assurance and cyber security.

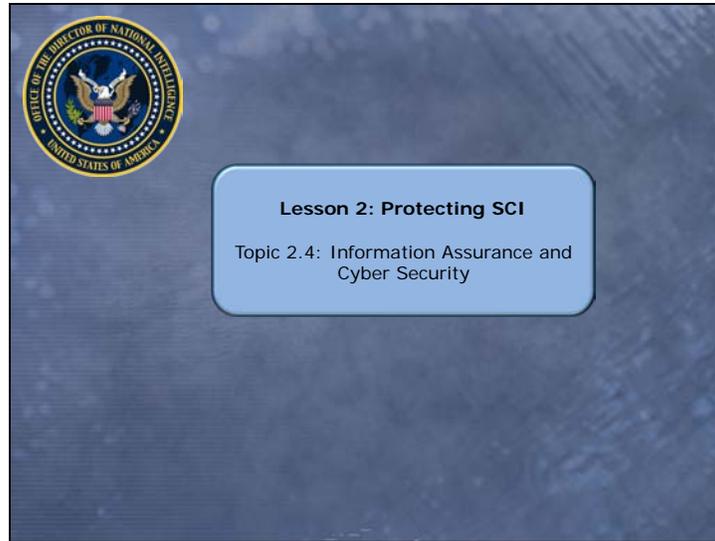
Summary

Physical and technical security methods include measures such as formal access controls, locks, SCIFs, and alarms. These measures are put in place to protect personnel, facilities, equipment, materials, and documents. A SCIF is a specially designed location with physical and technical security elements that allow it to be certified and accredited by the DNI for the processing, storage, and discussion of SCI. As a cleared professional, it is critical that you understand the policies and procedures for a SCIF, including:

- Locking and alarming
- Opening and closing
- Controlling access
- Escorting
- Holding classified discussions
- Handling materials
- Evacuating

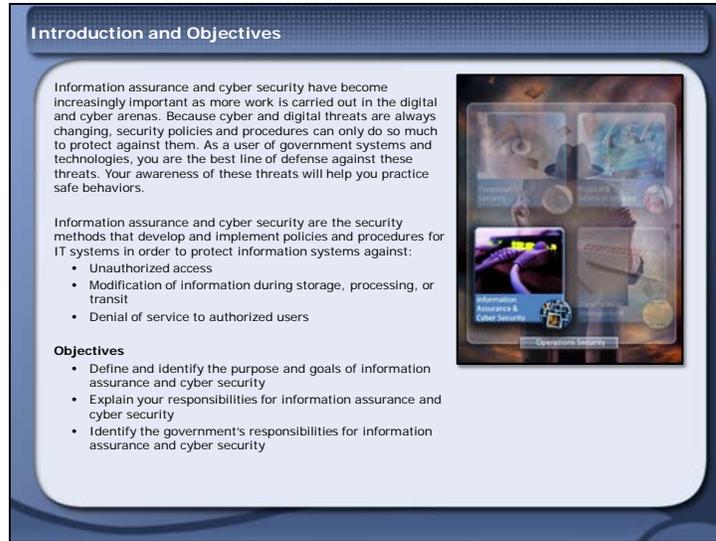
In addition, there are special rules for the proper use of phones and other telecommunication equipment of which you must be aware. Never take a phone, PED, or other two-way communication device into a SCIF.

In the next topic, you will discuss information assurance and cyber security. You will also learn your responsibilities and the government's responsibilities in relation to information assurance and cyber security.



Lesson 2: Protecting SCI

Topic 2.4: Information Assurance and Cyber Security



Introduction and Objectives

Information assurance and cyber security have become increasingly important as more work is carried out in the digital and cyber arenas. Because cyber and digital threats are always changing, security policies and procedures can only do so much to protect against them. As a user of government systems and technologies, you are the best line of defense against these threats. Your awareness of these threats will help you practice safe behaviors.

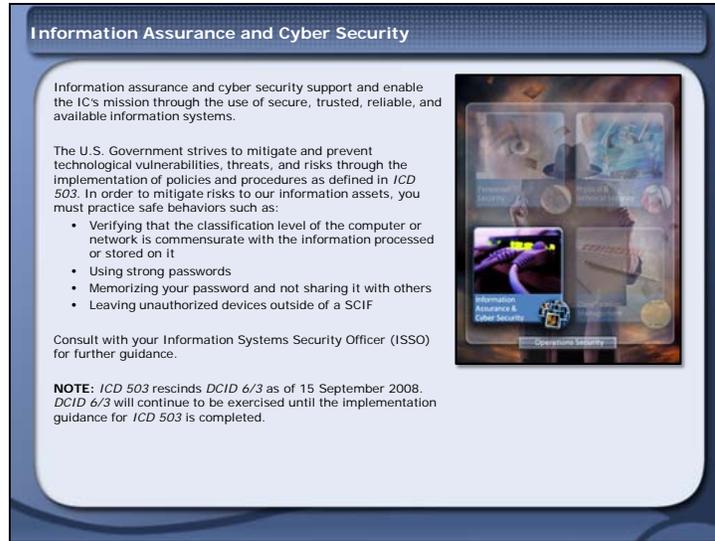
Information assurance and cyber security are the security methods that develop and implement policies and procedures for IT systems in order to protect information systems against:

- Unauthorized access
- Modification of information during storage, processing, or transit
- Denial of service to authorized users

Objectives

- Define and identify the purpose and goals of information assurance and cyber security
- Explain your responsibilities for information assurance and cyber security
- Identify the government's responsibilities for information assurance and cyber security

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification management surrounded by Operations Security; Information Assurance & Cyber Security is emphasized)



Information Assurance and Cyber Security

Information assurance and cyber security support and enable the IC's mission through the use of secure, trusted, reliable, and available information systems.

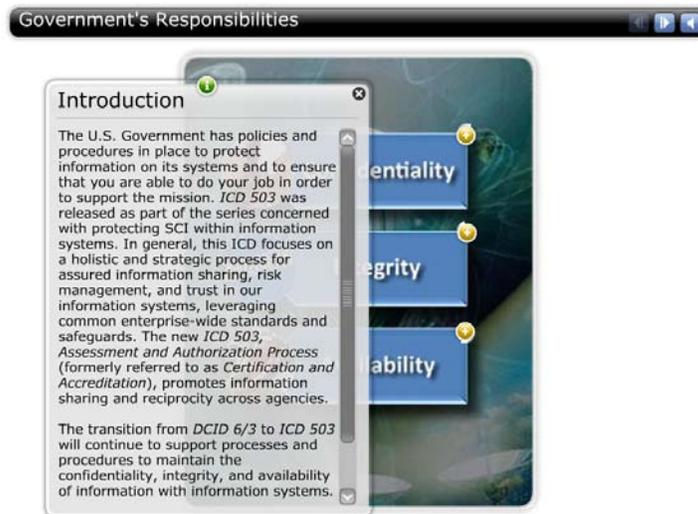
The U.S. Government strives to mitigate and prevent technological vulnerabilities, threats, and risks through the implementation of policies and procedures as defined in *ICD 503*. In order to mitigate risks to our information assets, you must practice safe behaviors such as:

- Verifying that the classification level of the computer or network is commensurate with the information processed or stored on it
- Using strong passwords
- Memorizing your password and not sharing it with others
- Leaving unauthorized devices outside of a SCIF

Consult with your Information Systems Security Officer (ISSO) for further guidance.

NOTE: *ICD 503* rescinds *DCID 6/3* as of 15 September 2008. *DCID 6/3* will continue to be exercised until the implementation guidance for *ICD 503* is completed.

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification management surrounded by Operations Security; Information Assurance & Cyber Security is emphasized)



Government's Responsibilities

Introduction

The U.S. Government has policies and procedures in place to protect information on its systems and to ensure that you are able to do your job in order to support the mission. *ICD 503* was released as part of the series concerned with protecting SCI within information systems. In general, this ICD focuses on a holistic and strategic process for assured information sharing, risk management, and trust in our information systems, leveraging common enterprise-wide standards and safeguards. The new *ICD 503, Assessment and Authorization Process* (formerly referred to as *Certification and Accreditation*) promotes information sharing and reciprocity across agencies.

The transition from *DCID 6/3* to *ICD 503* will continue to support processes and procedures to maintain the confidentiality, integrity, and availability of information with information systems.

Select the (+) by each term from the graphic to learn more.

(Image Alt: Collage of satellites, a person whispering, an "Integrity" label, and a hand picking an apple from a tree)

Confidentiality

The assurance that information is not accessible to:

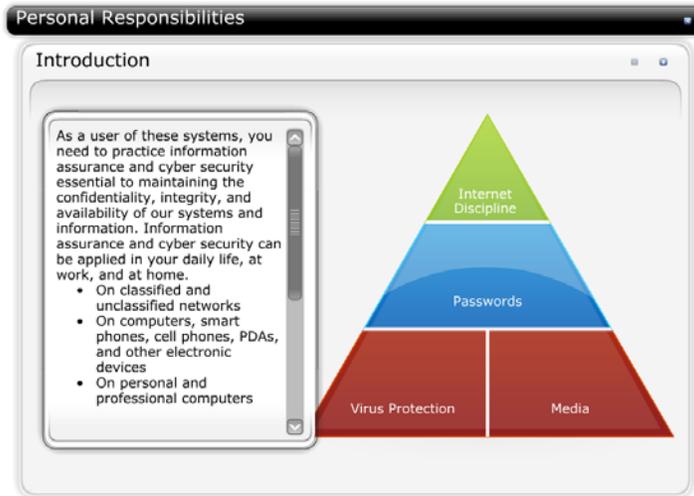
- Unauthorized individuals
- Processes
- Devices

Integrity

The assurance that information is protected against unauthorized modification or destruction.

Availability

The assurance that information is available and accessible when needed.



Personal Responsibilities

Introduction

As a user of these systems, you need to practice information assurance and cyber security essential to maintaining the confidentiality, integrity, and availability of our systems and information. Information assurance and cyber security can be applied in your daily life, at work, and at home. They can be applied on the following:

- Classified and unclassified networks
- Smart phones, cell phones, PDAs, and other electronic devices
- Personal and professional computers

Cyber threats to our information and information systems are continuously intensifying and becoming more complex. It is important that you follow information assurance and cyber security policies and guidelines for the appropriate use of:

- Media
- Passwords
- Virus protection
- Internet

Select each section of the pyramid to learn more about good security behaviors.

(Image Alt: A pyramid with three levels: Internet Discipline; Passwords; Virus Protection, Media)

Internet Discipline

If you are working in a classified environment, chances are you don't have easy access to the Internet, or if you do, you must change the system you are working on to access an unclassified environment. Regardless, if you are using the Internet at work or at home, it is essential that you practice good Internet discipline and keep in mind the following recommendations:

- Remember that the Internet is an **UNCLASSIFIED** communication system; don't talk about, or around, classified information

- Remember, there is no privacy or anonymity on the Internet; you do not know who is monitoring you
- Remember, you cannot be sure who is on the receiving end of your communication
- Remember to use classified communication systems to discuss sensitive information
- Think about the type of information you send or post on the Internet (i.e., via email, blog, tweet, social networking sites) and what it says about you and your classified work

The government has invested a significant amount of money and research in creating a safe and secure classified environment for your work. Use this system whenever possible.

NOTE: Be mindful of personal information that you provide outside of your work life.

Passwords

Protecting your passwords is important. They identify you as an authorized user and allow you access to read, modify, or manipulate information. Use the following sound security practices regarding your passwords:

- Memorize passwords and do not share them with others
- Build strong, smart passwords in accordance with your organization's policies
- Change your password frequently

NOTE: You may write a password down if it is stored within a secured safe within a SCIF.

Virus Protection

Protecting your system against viruses is essential. Viruses and other malware can damage the integrity of your information and system by copying or installing programs without permission and monitoring or controlling your system. A compromise of this type could have grave consequences to national security. Practice the following behaviors to minimize the risk of viruses:

- Follow your organization's guidance
- Have the ISSO scan **all** incoming media for viruses including new media (e.g., software) that is unopened/shrink-wrapped

If you think your system is infected by a virus, do the following:

- Discontinue any and all activities on your machine
- Contact your ISSO immediately

Media

Following responsible media security practices is essential in ensuring that "corrupt" files or adware are not introduced to your workstation or system. You should practice the following:

- Ensure that all media is marked with a classification level - use an indelible pen to write on Compact Discs (CD) and ask your ISSO for classification stickers to put on CD cases and boxes

- Have **all** new media (e.g., CDs, disks, software) virus-scanned prior to using it on your system
- Have your ISSO load all scanned media onto your system
- Remember that the only way to sanitize media is to "demagnetize" it
- Remember "Once in a SCIF, always in a SCIF"

NOTE: This means that once you introduce something to the classified environment, it becomes classified at the highest level. For example, if you put an **UNCLASSIFIED** CD into a **TOP SECRET** computer, the CD becomes classified at the **TOP SECRET** level even though no content on it has changed.



Knowledge Check - Information Assurance and Cyber Security

1. Information assurance and cyber security covers many different areas.

Review the list of activities. Select all that are *compliant* with information assurance and cyber security policies and then select SUBMIT.

Choice
Bringing a one-way pager into a SCIF
Bringing a cell phone into a SCIF
Loading new, still shrink-wrapped, software onto your work computer
Alluding to classified information on the Internet
Talking around classified information when using Internet email, social networking sites (e.g., Facebook), or text messaging from a cell phone
Giving your ISSO a CD or other removable media for virus/malware scanning prior to introduction to any system
Handling an UNCLASSIFIED CD that has been used on a TOP SECRET system as TOP SECRET

The following table reflects the correct answers.

Correct	Choice
	Bringing a one-way pager into a SCIF
	Bringing a cell phone into a SCIF
	Loading new, still shrink-wrapped, software onto your work computer
	Alluding to classified information on the Internet
	Talking around classified information when using Internet email, social networking sites (e.g., Facebook), or text messaging from a cell phone
X	Giving your ISSO a CD or other removable media for virus/malware scanning prior to introduction to any system
X	Handling an UNCLASSIFIED CD that has been used on a TOP SECRET system as TOP SECRET

Feedback when correct:

That's right! You selected the correct responses.

The following activities are compliant with information assurance and cyber security policies.

- Handling an **UNCLASSIFIED** CD that has been used on a **TOP SECRET** system as **TOP SECRET**
- Giving your ISSO a CD or other removable media for virus/malware scanning prior to introduction to any system

The following are security incidents under information assurance and cyber security:

- Loading new software onto your computer
- Alluding to classified information on the Internet

The cell phone, telephone, and pager options are part of physical and technical security. With the exception of the one way pager, they are examples of security incidents.

Feedback when incorrect:

You did not select the correct responses.

The following activities are compliant with information assurance and cyber security policies.

- Handling an **UNCLASSIFIED** CD that has been used on a **TOP SECRET** system as **TOP SECRET**
- Giving your ISSO a CD or other removable media for virus/malware scanning prior to introduction to any system

The following are security incidents under information assurance and cyber security:

- Loading new software onto your computer
- Alluding to classified information on the Internet

The cell phone, telephone, and pager options are part of physical and technical security. With the exception of the one way pager, they are examples of security incidents.

Summary

More work is being completed today in the digital and cyber arenas. *ICD 503* was put in place to promote information sharing and reciprocity across agencies; it emphasizes the confidentiality and integrity of information while maintaining its availability.

It is crucial that you are aware of, and always on the alert for, constantly changing digital and cyber threats. You can help to thwart these attacks by following established information assurance and cyber security policies and procedures such as:

- Following appropriate Internet discipline
- Using strong passwords
- Installing virus protection on your computer
- Properly using classified systems
- Appropriately marking and handling media

In the next topic you will examine your responsibilities in relation to classification management.



Summary

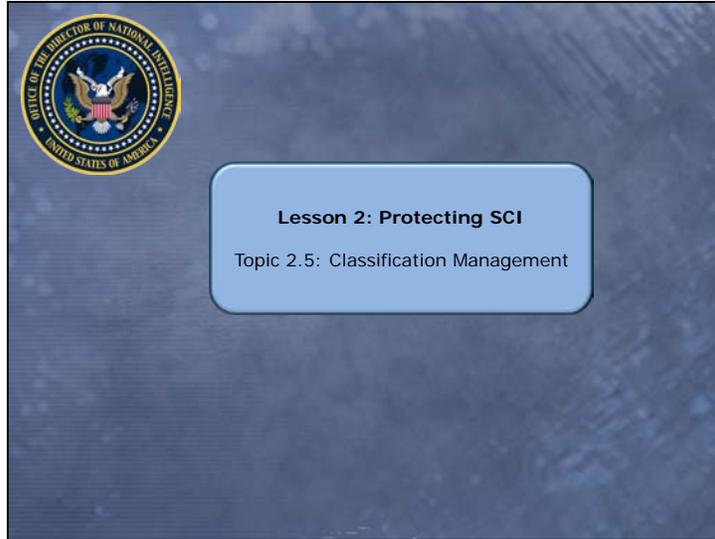
More work is being completed today in the digital and cyber arenas. *ICD 503* was put in place to promote information sharing and reciprocity across agencies; it emphasizes the confidentiality and integrity of information while maintaining its availability.

It is crucial that you are aware of, and always on the alert for, constantly changing digital and cyber threats. You can help to thwart these attacks by following established information assurance and cyber security policies and procedures such as:

- Following appropriate Internet discipline
- Using strong passwords
- Installing virus protection on your computer
- Properly using classified systems
- Appropriately marking and handling media

In the next topic you will examine your responsibilities in relation to classification management.

(Image Alt: Collage of a puzzle, a **TOP SECRET** folder, a **CONFIDENTIAL** document, and a keyboard)



Lesson 2: Protecting SCI

Topic 2.5: Classification Management

Introduction and Objectives

Classification Management is the process of determining and assigning classification and control markings, as appropriate, to classified and unclassified national intelligence.

The classification and control markings system is a critical element of IC procedures for:

- Protecting national intelligence information
- Protecting sources and methods
- Ensuring that information is available to authorized recipients without delay or unnecessary restrictions

Objectives

- Define and identify the purpose of classification management
- Explain your responsibilities for handling and marking classified information
- Identify the various components required for properly marking a classified document

Guidance on the classification management requirements can be found in *EO 13526, Classified National Security Information, 32 CFR Part 2001, Classified National Security Information; Final Rule*.

Guidance on the classification and control markings system can be found in *ICD 710, Classification and Control Markings System*.



Introduction and Objectives

Classification Management is the process of determining and assigning classification and control markings, as appropriate, to classified and unclassified national intelligence.

The classification and control markings system is a critical element of IC procedures for:

- Protecting national intelligence information
- Protecting sources and methods
- Ensuring that information is available to authorized recipients without delay or unnecessary restrictions

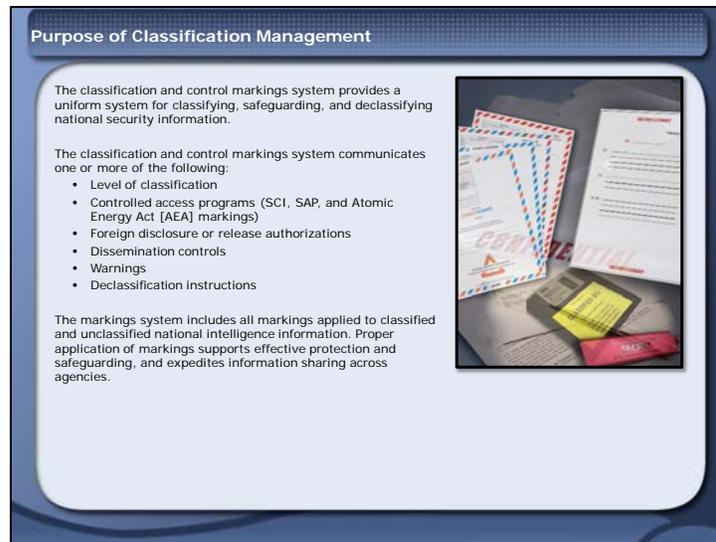
Objectives

- Define and identify the purpose of classification management
- Explain your responsibilities for handling and marking classified information
- Identify the various components required for properly marking a classified document
-

Guidance on the classification management requirements can be found in *EO 13526, Classified National Security Information, 32 CFR Part 2001, Classified National Security Information; Final Rule*.

Guidance on the classification and control markings systems can be found in *ICD 710, Classification and Control Markings System*.

(Image Alt: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification Management surrounded by Operations Security; Classification Management is emphasized)



Purpose of Classification Management

The classification and control markings system provides a uniform system for classifying, safeguarding, and declassifying national security information.

The classification and control markings system communicates one or more of the following:

- Level of classification
- Controlled access programs (SCI, SAP, and Atomic Energy Act [AEA] markings)
- Foreign disclosure or release authorizations
- Dissemination controls
- Warnings
- Declassification instructions

The markings system includes all markings applied to classified and unclassified national intelligence information. Proper application of markings supports effective protection and safeguarding, and expedites information sharing across agencies.

(Image Alt: Collage of properly marked documents and a properly marked disk and thumb drive)

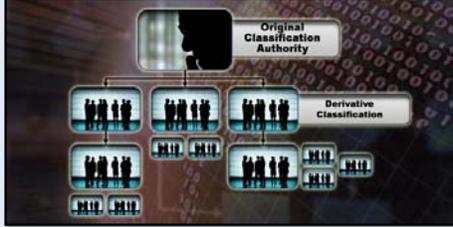
Classification Authorities

There are two types of classification authority:

- Original Classification Authority (OCA)
- Derivative classification authority

All information is initially classified by an OCA – a very small number of senior leaders.

You, as a cleared professional, are a derivative classifier. Derivative classifiers reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides. Derivative classifiers are responsible for assuring that information is appropriately classified and marked.



Classification Authorities

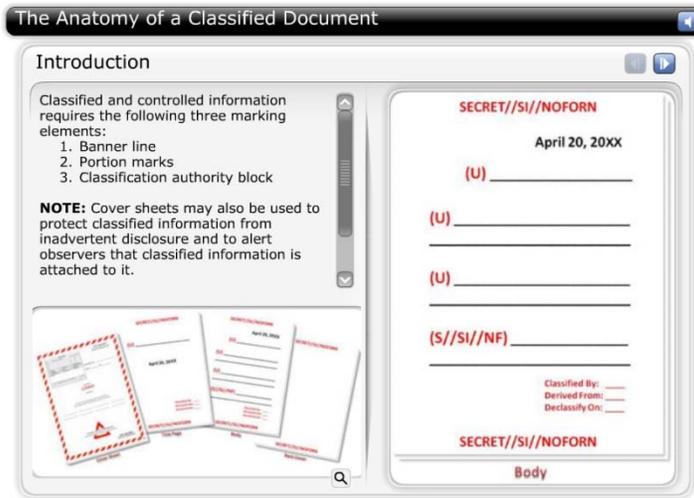
There are two types of classification authority:

- Original Classification Authority (OCA)
- Derivative classification authority

All information is initially classified by an OCA – a very small number of senior leaders.

You, as a cleared professional, are a derivative classifier. Derivative classifiers reproduce, extract, and summarize classified information, and apply classification markings derived from source material or classification guides. Derivative classifiers are responsible for assuring that information is appropriately classified and marked.

(Image Alt: A flow of classification authority from one OCA to many potential Derivative Classifiers)



The Anatomy of a Classified Document

Introduction

Classified and controlled information requires the following three marking elements:

1. Banner line
2. Portion marks
3. Classification authority block

NOTE: Cover sheets may also be used to protect classified information from inadvertent disclosure and to alert observers that classified information is attached to it.

Use the arrow buttons at the top to learn more about the anatomy of a classified document.

(Image Alt: A properly marked document including a cover sheet, title page, body, and back cover)

Banner Line

The banner line (header/footer) designates the overall classification and all applicable control markings of the document. The banner reflects the highest classification and most restrictive control markings of the individual portions.

In this case, the document is classified at the **SECRET** level and contains information protected in the **COMINT** Control System. It cannot be released to foreign nationals (**NOFORN**).

NOTE: All classified information, under the purview of *ICD 710*, shall contain the appropriate foreign release/disclosure markings at the portion and banner level.

Portion Marks

A portion mark must be applied to all classified and controlled information. Portion marks reflect the highest classification level and most restrictive control markings of each portion.

They are placed at the beginning of all portions, immediately preceding the text to which it applies. In this case, the information in the portion is:

- Classified **SECRET (S)**
- Controlled within the **COMINT** formal access control system (**SI**)
- Not eligible for release to foreign nationals (**NF**)

Classification Authority Block

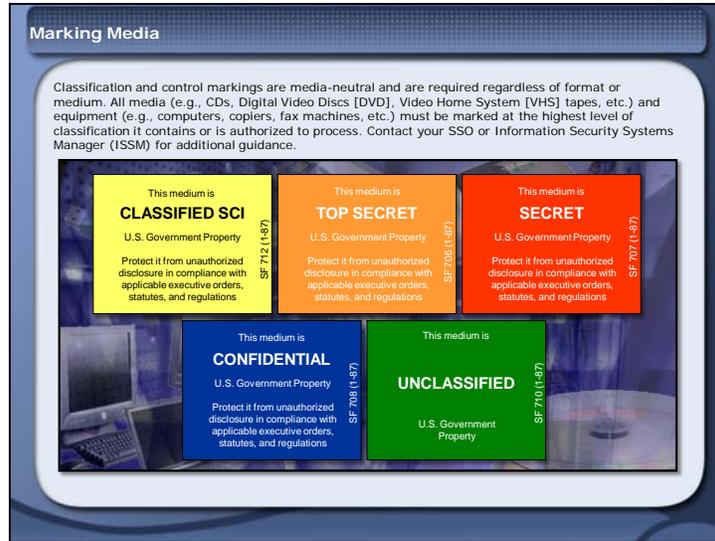
The classification authority block must be placed on the front cover or the first page of a classified document.

There are two forms of authority blocks:

- OCA
- Derivative classification authority

As a derivative classifier, your classification authority block will contain the following information:

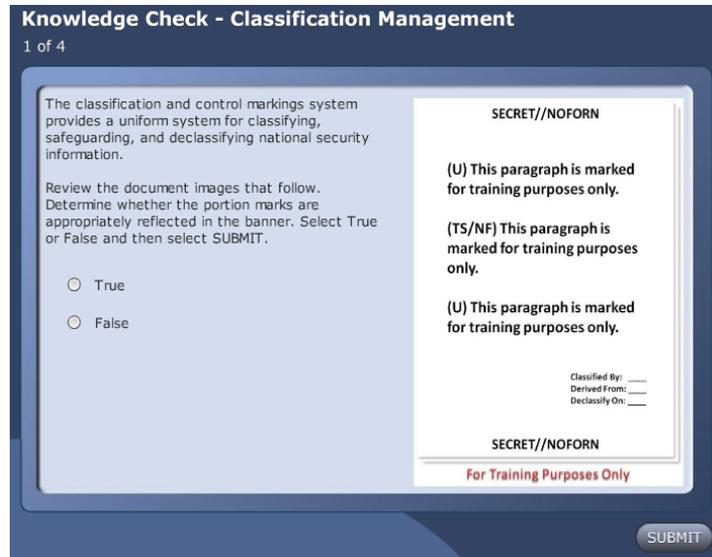
- Classified By: (Identity of person applying markings)
- Derived From: (Source of derivative classification)
- Declassify On: (Declassification instructions)



Marking Media

Classification and control markings are media-neutral and are required regardless of format or medium. All media (e.g., CDs, Digital Video Discs [DVD], Video Home System [VHS] tapes, etc.) and equipment (e.g., computers, copiers, fax machines, etc.) must be marked at the highest level of classification it contains or is authorized to process. Contact your SSO or Information Security Systems Manager (ISSM) for additional guidance.

(Image Alt: Collage of computers equipment and storage devices overlaid with five classification labels: **CLASSIFIED SCI**, **TOP SECRET**, **SECRET**, **CONFIDENTIAL**, **UNCLASSIFIED**)



Knowledge Check - Classification Management

1. The classification and control markings system provides a uniform system for classifying, safeguarding, and declassifying national security information.

Review the document images that follow. Determine whether the portion marks are appropriately reflected in the banner. Select True or False and then select SUBMIT.

SECRET//NOFORN

(U) This paragraph is marked for training purposes only.

(TS//NF) This paragraph is marked for training purposes only.

(U) This paragraph is marked for training purposes only.

Classified By: _____
Derived From: _____
Declassify On: _____

SECRET//NOFORN

Choice
True
False

The following table reflects the correct answer.

Correct	Choice
	True
X	False

Feedback when correct:

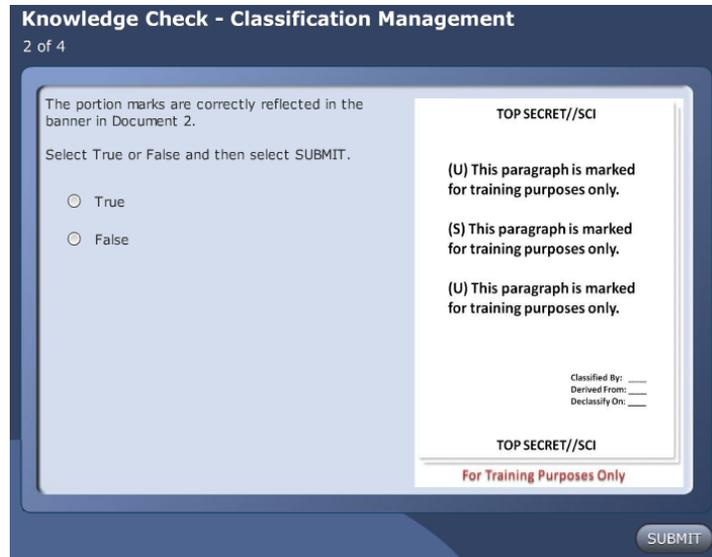
That's right! You selected the correct response.

Document 1 is incorrectly marked because the **SECRET** banner does not reflect the **TS** portion in the document.

Feedback when incorrect:

You did not select the correct response.

Document 1 is incorrectly marked because the **SECRET** banner does not reflect the **TS** portion in the document.



2. The portion marks are correctly reflected in the banner in Document 2.

Select True or False and then select SUBMIT.

TOP SECRET//SCI

(U) This paragraph is marked for training purposes only.

(S) This paragraph is marked for training purposes only.

(U) This paragraph is marked for training purposes only.

Classified By: _____

Derived From: _____

Declassify On: _____

TOP SECRET//SCI

Choice
True
False

The following table reflects the correct answer.

Correct	Choice
	True
X	False

Feedback when correct:

That's right! You selected the correct response.

The banner in Document 2 is incorrect for several reasons:

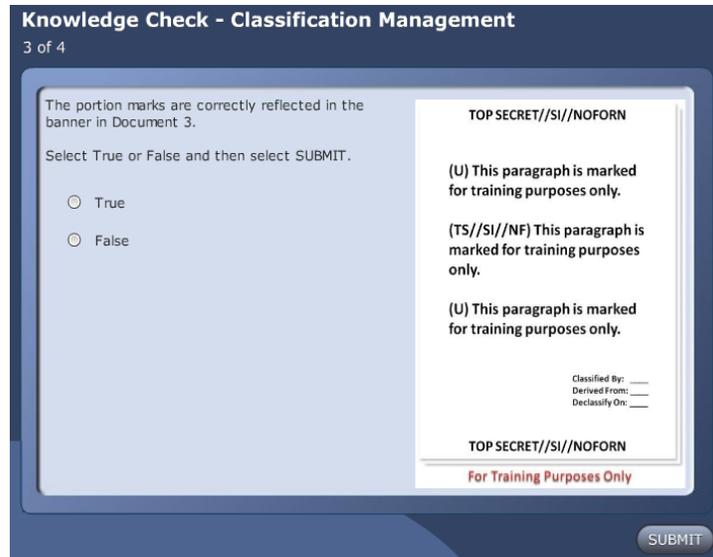
1. The highest classification level in a portion is **SECRET**, but the banner is marked **TOP SECRET**.
2. The banner indicates the presence of **SCI**; however, "**SCI**" is not an authorized marking.
3. The banner and portion marks do not contain foreign release/disclosure markings, as required by *ICD 710*.

Feedback when incorrect:

You did not select the correct response.

The banner in Document 2 is incorrect for several reasons:

1. The highest classification level in a portion is **SECRET**, but the banner is marked **TOP SECRET**.
2. The banner indicates the presence of **SCI**; however, "**SCI**" is not an authorized marking.
3. The banner and portion marks do not contain foreign release/disclosure markings, as required by *ICD 710*.



3. The portion marks are correctly reflected in the banner in Document 3.

Select True or False and then select SUBMIT.

TOP SECRET//SI//NOFORN

(U) This paragraph is marked for training purposes only.

(TS//SI//NF) This paragraph is marked for training purposes only.

(U) This paragraph is marked for training purposes only.

Classified By: _____

Derived From: _____

Declassify On: _____

TOP SECRET// SI//NOFORN

Choice
True
False

The following table reflects the correct answer.

Correct	Choice
X	True
	False

Feedback when correct:

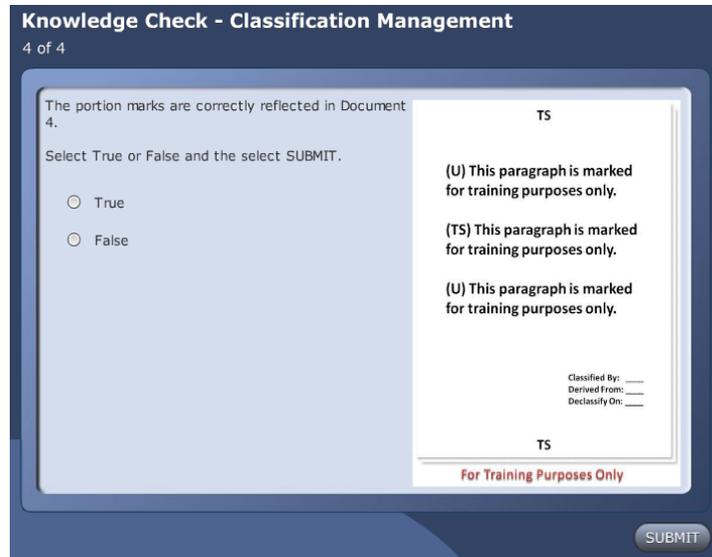
That's right! You selected the correct response.

The banner is correct in Document 3. The classification level (**TOP SECRET**), SAP (**SI**), and appropriate foreign release marking (**NOFORN**) in the banner accurately reflect the highest classification level and control markings in the portions.

Feedback when incorrect:

You did not select the correct response.

The banner is correct in Document 3. The classification level (**TOP SECRET**), SAP (**SI**), and appropriate foreign release marking (**NOFORN**) in the banner accurately reflect the highest classification level and control markings in the portions.



4. The portion marks are correctly reflected in Document 4.

Select True or False and the select SUBMIT.

TS

(U) This paragraph is marked for training purposes only.

(TS) This paragraph is marked for training purposes only.

(U) This paragraph is marked for training purposes only.

Classified By: _____

Derived From: _____

Declassify On: _____

TS

Choice
True
False

The following table reflects the correct answer.

Correct	Choice
	True
X	False

Feedback when correct:

That's right! You selected the correct response.

The banner in Document 4 is incorrect for two reasons:

1. **TOP SECRET** is not spelled out in the banner lines.
2. The banner lines and portion marks do not contain foreign release/disclosure markings, as required by *ICD 710*.

Feedback when incorrect:

You did not select the correct response.

The banner in Document 4 is incorrect for two reasons:

1. **TOP SECRET** is not spelled out in the banner lines.
2. The banner lines and portion marks do not contain foreign release/disclosure markings, as required by *ICD 710*.



Summary

Classification Management is the **process of determining and assigning** the appropriate classification and control markings to classified and unclassified national intelligence.

The classification and control markings **system** is a critical element for protecting intelligence and information while ensuring that information is available without delay or unnecessary restrictions. The markings system includes all markings applied to classified and unclassified national intelligence information. Proper application of markings supports effective protection and safeguards and expedites information sharing.

As an authorized holder of classified national intelligence and a derivative classifier, you are responsible for properly applying the following markings to national intelligence information:

- Banner line
- Portion marks
- Classification authority block

All media and equipment must be marked at the highest level of classification it contains or is authorized to process.

In the next topic, you will learn about some additional responsibilities that you must meet related to your personal activities.

Summary

Classification Management is the **process of determining and assigning** the appropriate classification and control markings to classified and unclassified national intelligence.

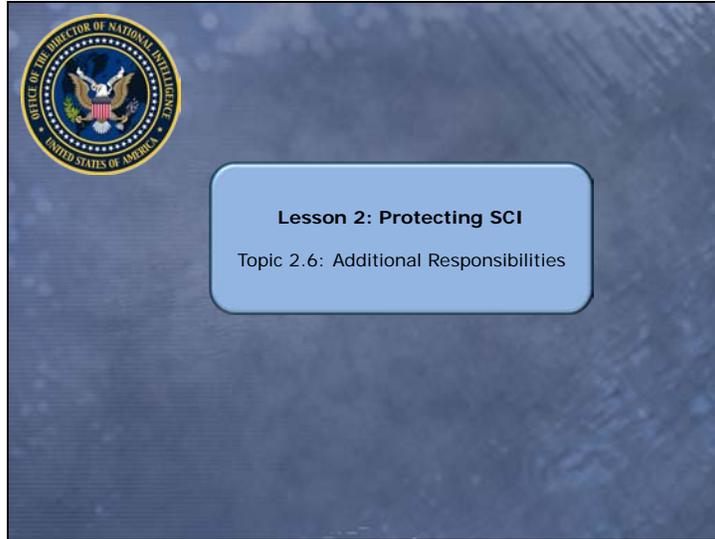
The classification and control markings **system** is a critical element for protecting intelligence and information while ensuring that information is available without delay or unnecessary restrictions. The markings system includes all markings applied to classified and unclassified national intelligence information. Proper application of markings supports effective protection and safeguards and expedites information sharing.

As an authorized holder of classified national intelligence and a derivative classifier, you are responsible for properly applying the following markings to national intelligence information:

- Banner line
- Portion marks
- Classification authority block

All media and equipment must be marked at the highest level of classification it contains or is authorized to process.

In the next topic, you will learn about some additional responsibilities that you must meet related to your personal activities.



Lesson 2: Protecting SCI

Topic 2.6: Additional Responsibilities

Introduction and Objectives

Going to school, volunteering, traveling, and/or engaging in social or athletic activities are just some activities that require you to balance your life at work and at home. Having a security clearance does not prohibit you from participating in these activities but it means that you must take precautions and abide by the following policies:

- Report unauthorized disclosures
- Conduct a pre-publication review
- Report security incidents and violations

Let us review your responsibilities regarding each of these.

Objectives

- Identify your additional reporting responsibilities to protect SCI
- Define an unauthorized disclosure and describe its potential effects
- Identify the general requirements needed to publish information in the public domain
- Describe the two categories of security incidents – violations and infractions



Introduction and Objectives

Going to school, volunteering, traveling, and/or engaging in social or athletic activities are just some activities that require you to balance your life at work and at home. Having a security clearance does not prohibit you from participating in these activities but it means that you must take precautions and abide by the following policies:

- Report unauthorized disclosures
- Conduct a pre-publication review
- Report security incidents and violations

Let us review your responsibilities regarding each of these.

Objectives

- Identify your additional reporting responsibilities to protect SCI
- Define an unauthorized disclosure and describe its potential effects
- Identify the general requirements needed to publish information in the public domain
- Describe the two categories of security incidents – violations and infractions

(Image Alt: Collage of a student carrying books, an office desk, a library and a group of volunteers)

Unauthorized Disclosures

You are responsible for protecting classified information from unauthorized disclosures. An unauthorized disclosure is a communication or physical transfer of national intelligence information, including SCI, to an unauthorized recipient. Unauthorized disclosures are a persistent problem and cause serious damage to national security and our intelligence capabilities. You must do your best to prevent them.

ICD 701 identifies policies regarding unauthorized disclosures and provides procedures to follow in the event of an unauthorized disclosure. *ICD 701*:

- Emphasizes the responsibilities of the IC to protect intelligence information
- Defines a process and establishes roles and responsibilities to deter, investigate, and promptly report unauthorized disclosures
- Ensures that appropriate protective and corrective actions are taken

NOTE: *ICD 701* (formerly *DCID 6/8*) was the first ICD signed by the DNI.

A photograph showing two individuals sitting on a park bench. One person is handing a bright red folder or document to the other. The scene is outdoors with trees in the background.

Unauthorized Disclosures

You are responsible for protecting classified information from unauthorized disclosures. An unauthorized disclosure is a communication or physical transfer of national intelligence information, including SCI, to an unauthorized recipient. Unauthorized disclosures are a persistent problem and cause serious damage to national security and our intelligence capabilities. You must do your best to prevent them.

ICD 701 identifies policies regarding unauthorized disclosures and provides procedures to follow in the event of an unauthorized disclosure. *ICD 701*:

- Emphasizes the responsibilities of the IC to protect intelligence information
- Defines a process and establishes roles and responsibilities to deter, investigate, and promptly report unauthorized disclosures
- Ensures that appropriate protective and corrective actions are taken

NOTE: *ICD 701* (formerly *DCID 6/8*) was the first ICD signed by the DNI.

(Image Alt: Two people sitting on a park bench passing a red folder)

Reporting Unauthorized Disclosures

If you become aware of, or suspect, an unauthorized disclosure of classified information, immediately notify your SSO and/or immediate supervisor. This notification requirement includes the intentional or accidental release or disclosure of classified information and the release of information to unauthorized recipients and through computer systems “spills.”

REMEMBER!

If you become aware of, or suspect, an unauthorized disclosure, security violation, or compromise of intelligence information, you should take the following measures:

- Gather your facts
- Promptly report your suspicions **only** to your immediate supervisor and SSO
- Use a secure system when reporting over electronic means (IT system or telephone)

Do not discuss this with anyone but your immediate supervisor and SSO.



Reporting Unauthorized Disclosures

If you become aware of, or suspect, an unauthorized disclosure of classified information, immediately notify your SSO and/or immediate supervisor. This notification requirement includes the intentional or accidental release or disclosure of classified information and the release of information to unauthorized recipients and through computer systems “spills.”

REMEMBER!

If you become aware of, or suspect, an unauthorized disclosure, security violation, or compromise of intelligence information, you should take the following measures:

- Gather your facts
- Promptly report your suspicions **only** to your immediate supervisor and SSO
- Use a secure system when reporting over electronic means (IT system or telephone)

Do not discuss this with anyone but your immediate supervisor and SSO.

(Image Alt: Collage of a person peaking from the shadows, a book, a newspaper, two people looking surprised, and a thought bubble reading “This can’t be right, I need to notify security immediately!”)

Pre-Publication Requirements

In accordance with *ODNI Instruction No.80.04*, all government information, whether classified or not, must have a release review before it can be made public.

As a cleared professional, you have an additional requirement pursuant to *ODNI Instruction No. 2007-6* and the Nda. You are required to submit for pre-publication review any information that you create for non-official purposes, if it is based on knowledge gained by your access to classified data. This review ensures that the information you create does not compromise any classified information or activity. The following are some examples of information that require a review:

- Speeches, articles, white papers, advertisements, etc.
- Web pages, web sites, blogs, chat rooms, video teleconferences, etc.

Contact your agency's pre-publication review office for more guidance. The ODNI Instruction can be found in the Course Resources.



REMEMBER!

Even if your resources are from open sources, if you realize the significance of that information from your classified access, the publication review still applies. Why? Because you may inadvertently give validity to the open-source information and compromise or expose sources or intelligence.

Pre-Publication Requirements

In accordance with *ODNI Instruction No.80.04*, all government information, whether classified or not, must have a release review before it can be made public.

As a cleared professional, you have an additional requirement pursuant to *ODNI Instruction No.2007-6* and the Nda. You are required to submit for pre-publication review any information that you create for non-official purposes, if it is based on knowledge gained by your access to classified data. This review ensures that the information you create does not compromise any classified information or activity. The following are some examples of information that require a review:

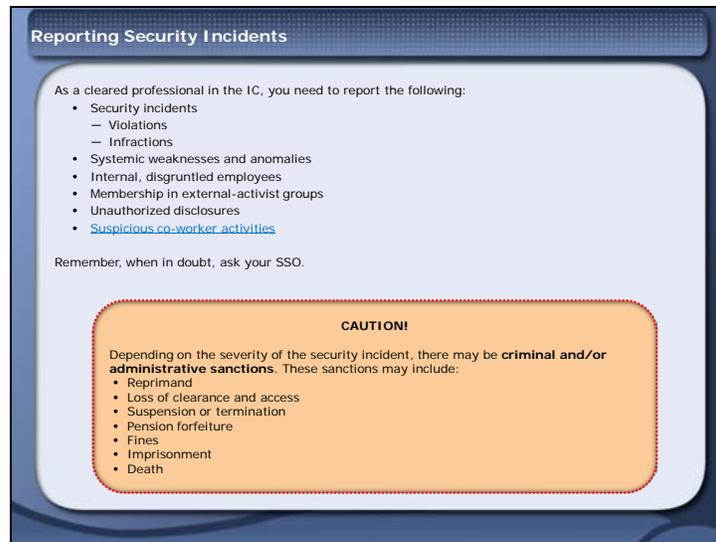
- Speeches, articles, white papers, advertisements, etc.
- Web pages, web sites, blogs, chat rooms, video teleconferences, etc.

Contact your agency's pre-publication review office for more guidance. The ODNI Instruction can be found in the Course Resources.

REMEMBER!

Even if your resources are from open sources, if you realize the significance of that information from your classified access, the publication review still applies. Why? Because you may inadvertently give validity to the open-source information and compromise or expose sources or intelligence.

(Image Alt: A hand reaching for a pen and contract while two reviewers hold up red and green signs)



Reporting Security Incidents

As a cleared professional in the IC, you need to report the following:

- Security incidents
- Violations
- Infractions
- Systemic weaknesses and anomalies
- Internal, disgruntled employees
- Membership in external-activist groups
- Unauthorized disclosures
- Suspicious co-worker activities

Remember, when in doubt, ask your SSO.

CAUTION!

Depending on the severity of the security incident, there may be **criminal and/or administrative sanctions**. These sanctions may include:

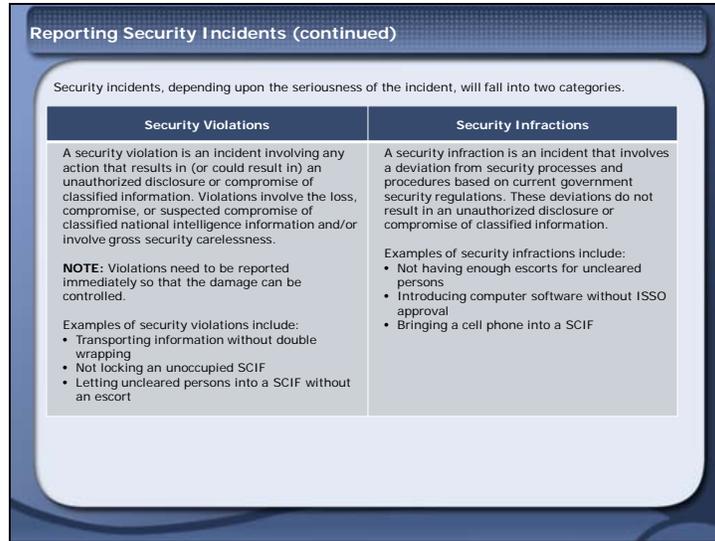
- Reprimand
- Loss of clearance and access
- Suspension or termination
- Pension forfeiture
- Fines
- Imprisonment
- Death

Suspicious Co-worker Activities (pop-up)

Suspicious co-worker activities are those in which you notice a coworker involved in security incidents (i.e., violations, infractions, or unauthorized disclosures) or unusual behaviors.

The following are some examples of suspicious co-worker activities:

- Conducting improper solicitations for information
- Having contact with the media
- Working odd hours by themselves
- Surfing classified sites that are not relevant to their work
- Using a thumb drive in a SCIF



Reporting Security Incidents (continued)

Security incidents, depending upon the seriousness of the incident, will fall into two categories.

Security Violations

A security violation is an incident involving any action that results in (or could result in) an unauthorized disclosure or compromise of classified information. Violations involve the loss, compromise, or suspected compromise of classified national intelligence information and/or involve gross security carelessness.

NOTE: Violations need to be reported immediately so that the damage can be controlled.

Examples of security violations include:

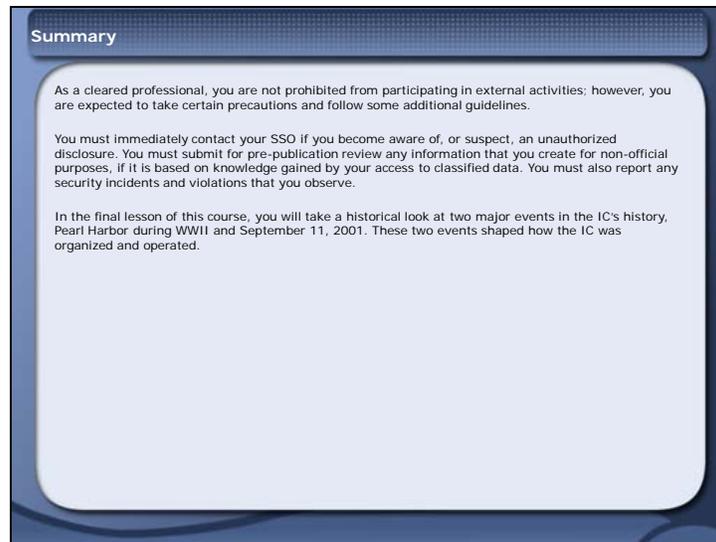
- Transporting information without double wrapping
- Not locking an unoccupied SCIF
- Letting uncleared persons into a SCIF without an escort

Security Infractions

A security infraction is an incident that involves a deviation from security processes and procedures based on current government security regulations. These deviations do not result in an unauthorized disclosure or compromise of classified information.

Examples of security infractions include:

- Not having enough escorts for uncleared persons
- Introducing computer software without ISSO approval
- Bringing a cell phone into a SCIF

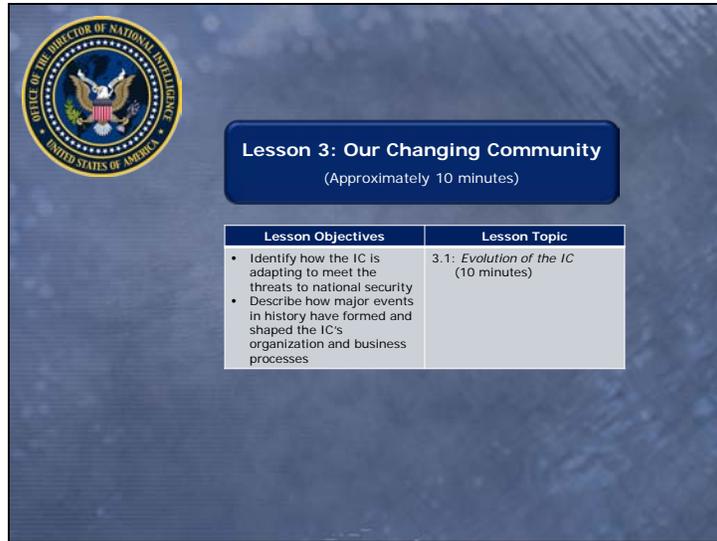


Summary

As a cleared professional, you are not prohibited from participating in external activities; however, you are expected to take certain precautions and follow some additional guidelines.

You must immediately contact your SSO if you become aware of, or suspect, an unauthorized disclosure. You must submit for pre-publication review any information that you create for non-official purposes, if it is based on knowledge gained by your access to classified data. You must also report any security incidents and violations that you observe.

In the final lesson of this course, you will take a historical look at two major events in the IC's history, Pearl Harbor during WWII and September 11, 2001. These two events shaped how the IC was organized and operated.



The slide features the Director of National Intelligence seal in the top left corner. The main title is "Lesson 3: Our Changing Community" with a subtitle "(Approximately 10 minutes)". Below this is a table with two columns: "Lesson Objectives" and "Lesson Topic".

Lesson Objectives	Lesson Topic
<ul style="list-style-type: none">Identify how the IC is adapting to meet the threats to national securityDescribe how major events in history have formed and shaped the IC's organization and business processes	3.1: <i>Evolution of the IC</i> (10 minutes)

Lesson 3: Our Changing Community

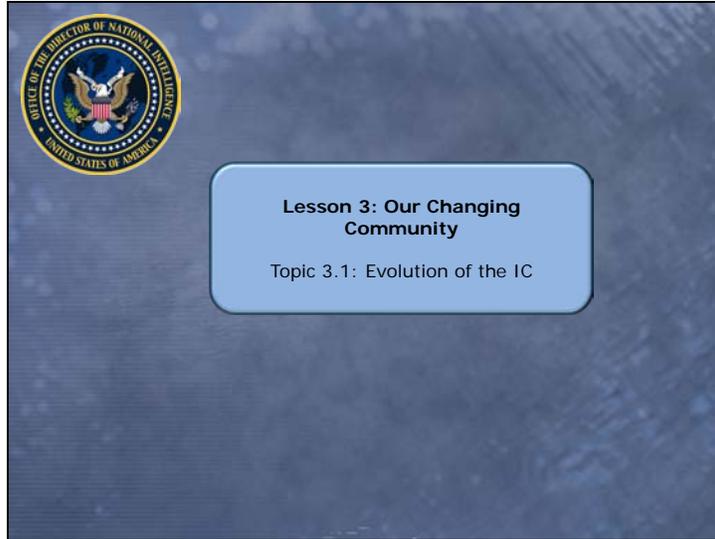
(Approximately 10 minutes)

Lesson Objectives

- Identify how the IC is adapting to meet the threats to national security
- Describe how major events in history have formed and shaped the IC's organization and business processes

Lesson Topic

3.1: *Evolution of the IC* (10 minutes)



Lesson 3: Our Changing Community

Topic 3.1: Evolution of the IC

Introduction and Objectives

To better understand the IC of today, it is necessary to understand its evolution over the years. Changes in the IC's structure, policies, and procedures occurred in response to historical attacks and emerging threats to the U.S.

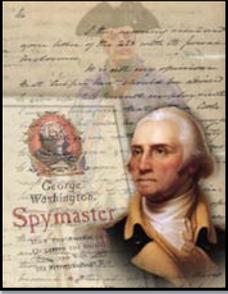
Prior to WWII, and even to 9/11, the IC was very different from the one of today. Learning the reasons for the IC's change over time will help us to avoid repeating past mistakes and allow the IC to continue to evolve in response to changing and emerging threats.

We will examine the pre- and post-WWII and post-9/11 events that were significant to the IC, and how the IC evolved in order to address threats to our national security.

Objectives

- Identify laws and policies that have been enacted to establish, define, and govern the IC
- Identify how the IC is adapting to meet current threats
- Describe how the events of 9/11 have impacted the IC and led to a change in focus and business practices

REMEMBER!
"Those who do not learn from history are doomed to repeat it."
- George Santayana, philosopher



Introduction and Objectives

To better understand the IC of today, it is necessary to understand its evolution over the years. Changes in the IC's structure, policies, and procedures occurred in response to historical attacks and emerging threats to the U.S.

Prior to WWII, and even to 9/11, the IC was very different from the one of today. Learning the reasons for the IC's change over time will help us to avoid repeating past mistakes and allow the IC to continue to evolve in response to changing and emerging threats.

We will examine the pre- and post-WWII and post-9/11 events that were significant to the IC, and how the IC evolved in order to address threats to our national security.

Objectives

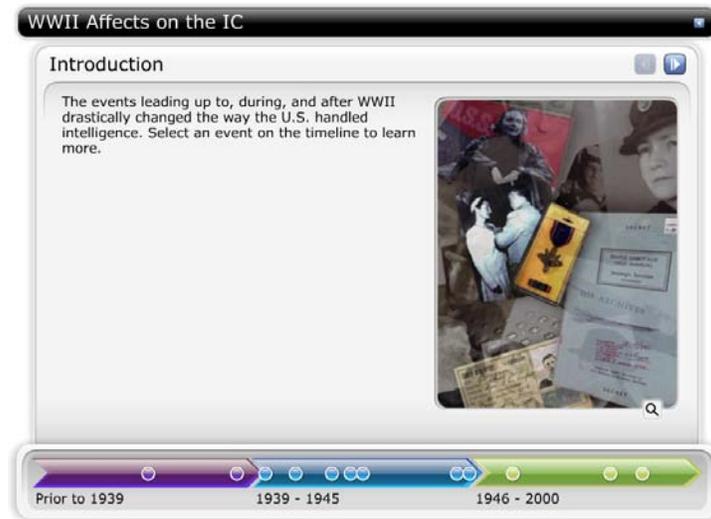
- Identify laws and policies that have been enacted to establish, define, and govern the IC
- Identify how the IC is adapting to meet current threats
- Describe how the events of 9/11 have impacted the IC and led to a change in focus and business practices

REMEMBER!

"Those who do not learn from history are doomed to repeat it."

-George Santayana, philosopher

(Image Alt: Collage of colonial soldier; George Washington; and a book, *Spymaster*)



WWII Affects on the IC

Introduction

The events leading up to, during, and after WWII drastically changed the way the U.S. handled intelligence. Select an event on the timeline to learn more.

(Image Alt: Collage of pre-WWII paraphernalia including, a medal, a field manual, an identification card, a sailor, a nurse, an OSS flag, and a typewriter)

Prior to 1939

Pre-WWII Intelligence Methodology (before 1939)

Before WWII there was no permanent IC. Cleared professionals followed very different security procedures than those of today. In fact, intelligence collection and protection efforts were simpler overall.

- The one classification level was **SECRET**
- The only formal, structured, intelligence collection effort was directed at collecting tactical intelligence during wartime
- No strategic intelligence organization existed and strategic intelligence capabilities were meager
- Intelligence organizations were temporary
- Intelligence collection efforts were fragmented and competitive

Breaking Japanese Codes (1938)

Throughout most of the early 20th century (prior to WWII), Japan was an expansionist nation seeking territory and resources. By 1938, the U.S. had broken Japanese diplomatic codes.

1939 - 1945

WWII Begins (1939)

September 1, 1939 was the official start of WWII when Germany invaded Poland.

Project ULTRA (1940)

Project ULTRA was the name used by the British for intelligence resulting from decryption of German radio communications during WWII (in the years 1940-1944). The decryption project was considered more sensitive than the highest security protection provided by the existing classification system. Therefore, a new system was put into place (e.g., compartments, code words, etc.). Project ULTRA became the basis for the U.S. Government's SCI security system.

Pearl Harbor (1941)

By 1941, based on collected information, the U.S. was anticipating an attack by the Japanese somewhere in the Pacific - possibly Hong Kong, Malaysia, or the Philippines. However, in a surprise attack on December 7, 1941, the Japanese Navy sent an aircraft carrier task force across the Pacific and bombed Pearl Harbor Naval Base in Hawaii.

The U.S. Government received warning of an imminent attack from intercepted diplomatic messages but had not broken the Japanese naval code. The Japanese naval code provided instructions to the Japanese fleet, including the attack location. As a result of their inability to decipher the code, the U.S. Government was unable to determine the exact attack location and was unable to warn the base. Because the U.S. Government had no strategic intelligence capability, no reliable information from other sources was available. Pearl Harbor Naval Base was taken completely by surprise, and the U.S. became involved in WWII.

Office of Strategic Services (OSS) Established (1942)

In response to the surprise attack on Pearl Harbor, U.S. intelligence collection and protection evolved. WWII presented the U.S. with the dual challenges of distance and magnitude in:

- Collecting, analyzing, and disseminating intelligence
- Protecting innovative and critical technical information
- Vetting foreign scientists for clearances
- Detecting and preventing unauthorized disclosures during classified projects

In June 1942, the U.S. formed the OSS to oversee the collection, analysis, and dissemination of intelligence. The OSS was the first true, integrated, strategic intelligence organization.

WWII intelligence initiatives changed intelligence gathering and classified security procedures. From these, a new IC organization and new security procedures for classified projects were created.

Manhattan Project (1942)

The Manhattan Project (1942-1946) was conducted to develop the first nuclear bomb. This was one of the first programs that brought together thousands of people from different nationalities to work on a single program that focused on developing new technologies and weaponry. The development locations were scattered throughout the U.S. The sensitivity and magnitude of this project demanded an integrated security program which included enhanced background checks of personnel and investigations of unauthorized disclosures. This was the

first time in our history that a comprehensive and disciplined security program was implemented.

WWII Ends (1945)

The end of WWII came in August 1945 with the unconditional surrender of Germany and Japan.

OSS Disbanded (1945)

In September 1945, the OSS was disbanded. This organization later provided the framework for the CIA.

1946 - 2000

National Security Act (1947)

The *National Security Act of 1947* remains the legal foundation of the IC. It mandated a major reorganization of the U.S. Government's national security structure and established the following entities:

- NSC
- Director of Central Intelligence (DCI)
- CIA

The *National Security Act of 1947* merged the War and Navy Departments into a single DoD, created a Department of the Air Force, and established the Secretary of Defense as the director of both. The following historical EOs further clarified IC responsibilities:

- *EO 11905* (1976)
- *EO 12333* (historical version 1981, amended in 2008)

Congress also set out to accomplish the following:

- Protect the civil liberties of U.S. persons by separating foreign and domestic intelligence
- Allow for collaboration between the agencies versus giving all the power to one agency

EO 11905 (1976)

EO 11905, signed by President Gerald R. Ford on February 18, 1976, established policies to improve the quality of intelligence needed for national security, clarified the authority and responsibilities of the intelligence departments and agencies, and established effective oversight to assure compliance with the law in the management and direction of intelligence agencies and departments of the national government.

IC components, at that time, included the following organizations:

- CIA
- NSA
- DIA
- Special offices within the DoD for the collection of specialized intelligence through reconnaissance programs

Separate intelligence elements also existed within the following:

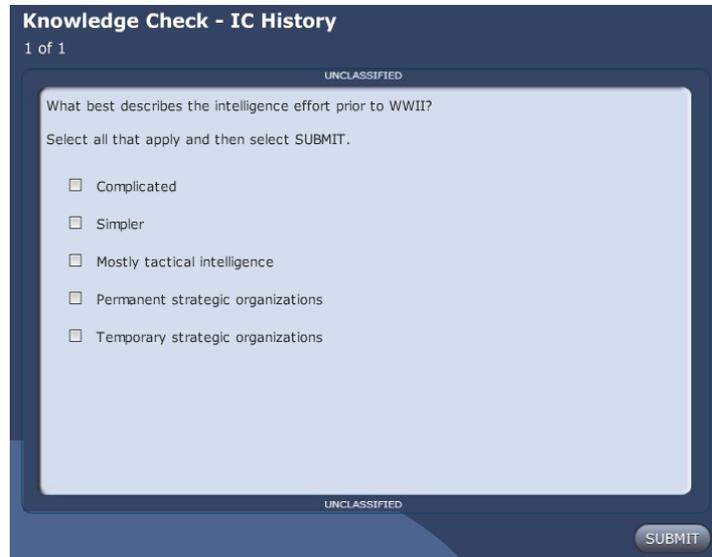
- Military services
- FBI
- DOS
- Department of the Treasury
- Energy Research and Development Administration

EO 12333 (1981)

EO 12333, signed by President Ronald Reagan on December 4, 1981 (amended in 2008), established the IC and charged it with the following:

- Collection of information needed by the President, the NSC, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities
- Production and dissemination of intelligence
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and/or narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons and their agents
- Special Activities
- Administrative and support activities within the U.S. and abroad as necessary for the performance of authorized activities
- Such other intelligence activities as the President may direct from time to time

EO 12333 also established prohibitions against certain intelligence activities such as assassination, collection against U.S. persons, and experimentation on humans without their knowledge.



Knowledge Check - IC History

1. What best describes the intelligence effort prior to WWII?

Select all that apply and then select SUBMIT.

Choice
Complicated
Simpler
Mostly tactical intelligence
Permanent strategic organizations
Temporary strategic organizations

The following table reflects the correct answers.

Correct	Choice
	Complicated
X	Simpler
X	Mostly tactical intelligence
	Permanent strategic organizations
X	Temporary strategic organizations

Feedback when correct:

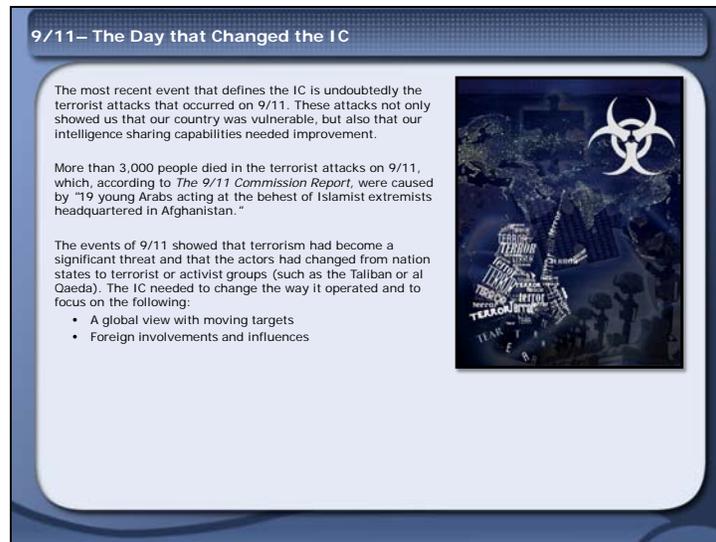
That's right! You selected the correct responses.

The intelligence effort prior to WWII was simpler and consisted of temporary organizations conducting tactical intelligence and limited strategic intelligence.

Feedback when incorrect:

You did not select the correct responses.

The intelligence effort prior to WWII was simpler and consisted of temporary organizations conducting tactical intelligence and limited strategic intelligence.



9/11– The Day that Changed the IC

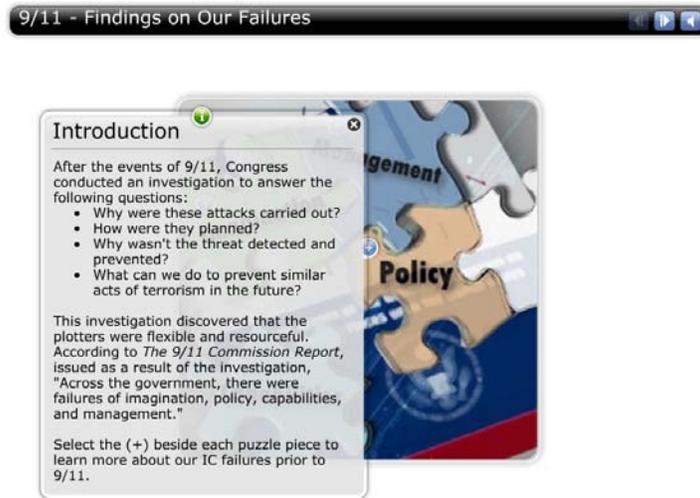
The most recent event that defines the IC is undoubtedly the terrorist attacks that occurred on 9/11. These attacks not only showed us that our country was vulnerable, but also that our intelligence sharing capabilities needed improvement.

More than 3,000 people died in the terrorist attacks on 9/11, which, according to *The 9/11 Commission Report*, were caused by "19 young Arabs acting at the behest of Islamist extremists headquartered in Afghanistan."

The events of 9/11 showed that terrorism had become a significant threat and that the actors had changed from nation states to terrorist or activist groups (such as the Taliban or al Qaeda). The IC needed to change the way it operated and to focus on the following:

- A global view with moving targets
- Foreign involvements and influences

(Image Alt: Collage of puzzle pieces; boots, guns, and helmets; a satellite image of Europe, Africa, and Asia; a weaponry/hazard symbol; and "Terror")



9/11 - Findings on Our Failures

Introduction

After the events of 9/11, Congress conducted an investigation to answer the following questions:

- Why were these attacks carried out?
- How were they planned?
- Why wasn't the threat detected and prevented?
- What can we do to prevent similar acts of terrorism in the future?

This investigation discovered that the plotters were flexible and resourceful. According to *The 9/11 Commission Report*, issued as a result of the investigation, "Across the government, there were failures of imagination, policy, capabilities, and management."

Select the (+) beside each puzzle piece to learn more about our IC failures prior to 9/11.

(Image Alt: Collage of the *9/11 Commission Report* and puzzle pieces labeled Management, Imagination, Policy, and Capabilities)

Imagination

We did not understand "...the gravity of the threat. The terrorist danger from Bin Ladin and al Qaeda was not a major topic for policy debate among the public, the media, or in the Congress.

Al Qaeda's new brand of terrorism presented challenges to U.S. governmental institutions that they were not well-designed to meet."

- *The 9/11 Commission Report, Executive Summary*

Al Qaeda and other terrorist organizations have proved very resilient and constantly adapt their tactics to overcome U.S. intelligence and security measures.

Management

Our government could not adapt the way it manages problems to the new challenges of the 21st Century.

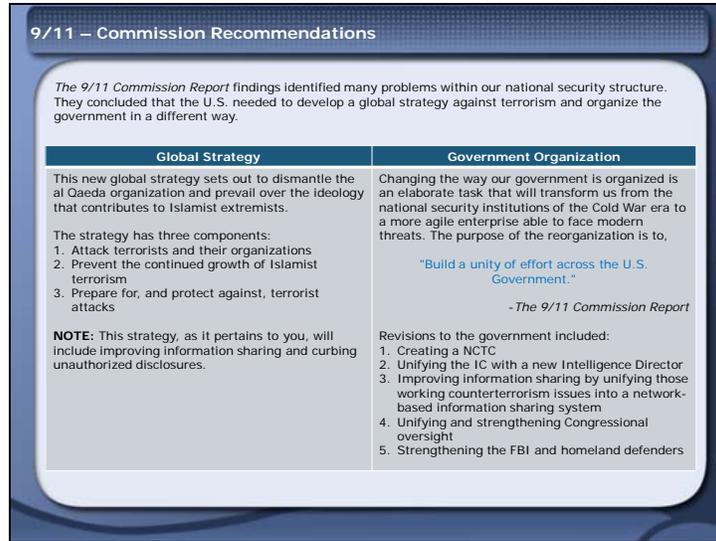
Policy

Prior to 9/11, terrorism was not an overriding national security concern for the U.S. Government. "The policy challenges were linked to this failure of imagination." Officials "...regarded a full U.S. invasion of Afghanistan as practically inconceivable before 9/11."

- *The 9/11 Commission Report, Executive Summary*

Capabilities

The IC was attempting to solve the al Qaeda problem with the same intelligence capabilities used during the Cold War.



9/11 – Commission Recommendations

The 9/11 Commission Report findings identified many problems within our national security structure. They concluded that the U.S. needed to develop a global strategy against terrorism and organize the government in a different way.

Global Strategy

This new global strategy sets out to dismantle the al Qaeda organization and prevail over the ideology that contributes to Islamist extremists.

The strategy has three components:

1. Attack terrorists and their organizations
2. Prevent the continued growth of Islamist terrorism
3. Prepare for, and protect against, terrorist attacks

NOTE: This strategy, as it pertains to you, will include improving information sharing and curbing unauthorized disclosures.

Government Organization

Changing the way our government is organized is an elaborate task that will transform us from the national security institutions of the Cold War era to a more agile enterprise able to face modern threats. The purpose of the reorganization is to,

"Build a unity of effort across the U.S. Government."

-The 9/11 Commission Report

Revisions to the government included:

1. Creating the NCTC
2. Unifying the IC with a new Intelligence Director

3. Improving information sharing by unifying those working counterterrorism issues into a network-based information sharing system
4. Unifying and strengthening Congressional oversight
5. Strengthening the FBI and homeland defenders

9/11 – Implications for Security

The *9/11 Commission Report* detailed IC flaws and made recommendations for mitigation. As a cleared professional working on issues of national security, you are now charged with the following tasks:

- Recognizing the expanding threat matrix
- Changing security perspectives
- Improving information sharing

These tasks led to the creation or modification of legislation and EOs, the development of an IC-wide vision, and a restructuring of the IC.



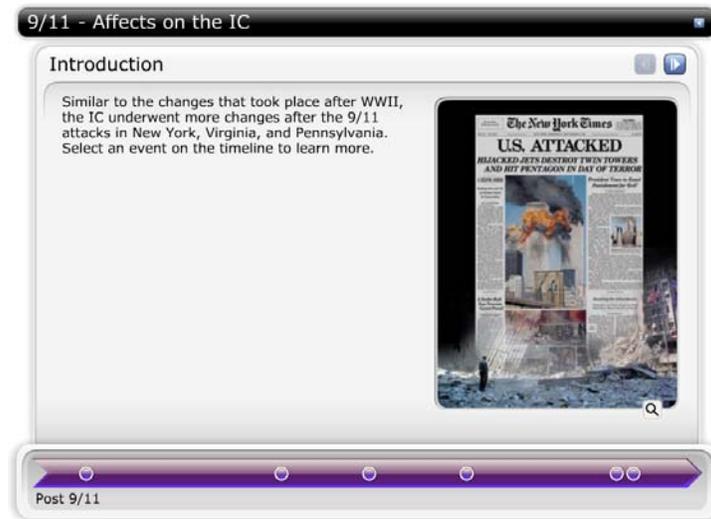
9/11 – Implications for Security

The *9/11 Commission Report* detailed IC flaws and made recommendations for mitigation. As a cleared professional working on issues of national security, you are now charged with the following tasks:

- Recognizing the expanding threat matrix
- Changing security perspectives
- Improving information sharing

These tasks led to the creation or modification of legislation and EOs, the development of an IC-wide vision, and a restructuring of the IC.

(Image Alt: Collage of a bay of lap top computers, people running from an explosion, and an opened door leading to a file room)



9/11 - Affects on the IC

Introduction

Similar to the changes that took place after WWII, the IC underwent more changes after the 9/11 attacks in New York, Virginia, and Pennsylvania. Select an event on the timeline to learn more.

(Image Alt: Collage of Ground Zero and the *New York Times* headline reading “U.S. Attacked, Hijacked Jets, Destroy Twin Towers and Hit Pentagon In Day of Terror”)

Post 9/11

9/11 Terror Attacks (2001)

On the morning of September 11, 2001, al Qaeda terrorists hijacked four commercial airlines in the U.S. Two were flown into the World Trade Center in New York City, NY; one was flown into the Pentagon in Arlington, VA; and one crashed near Shanksville, PA when several passengers over-powered the hijackers.

Intelligence Reform and Terrorism Prevention Act (2004)

The *IRTPA*, signed by President George W. Bush on December 17, 2004, significantly reformed the IC and intelligence-related activities of the U.S. Government.

The *IRTPA* is divided into eight titled subject areas:

1. Reform of the IC
2. FBI
3. Security Clearances
4. Transportation Security
5. Border Protection, Immigration, and Visa Matters
6. Terrorism Prevention
7. Implementation of 9/11 Commission Recommendations
8. Other Matters

National Intelligence Strategy (2005)

The *NIS*, implemented in 2005, describes the drastic overhaul in the U.S. IC, including the implementation of a new system for sharing information and the integration of existing enterprises to meet mission objectives and enterprise objectives. The legal basis for the *NIS* is the *IRTPA*.

The Mission Objectives described in the *NIS* aim to predict and prevent threats to U.S. national security and to assist all those who try to secure it. The following are the five Mission Objectives:

- Defeat terrorists
- Counter the spread of weapons of mass destruction
- Support democratic, or aspiring democratic, governments
- Improve existing analytical capabilities
- Increase the roll of strategic forecasting

The ten Enterprise Objectives describe the U.S.' capability to maintain a competitive advantage over elements that threaten the security of our nation. The ten Enterprise Objectives are:

- Increase the role of the Department of Justice (DoJ) within the community
- Create a new culture that promotes alternative viewpoints and uses expertise
- Optimize collection capabilities
- Hire result-focused employees with various skill sets
- Change the culture from 'need-to-know' to 'need-to-share'
- Increase cooperation among allies' intelligence services
- Create new uniform security practices
- Establish a uniform process for scientific and technological activities
- Create a reward system to promote competence
- Eliminate redundant systems while streamlining existing programs

National Intelligence Strategy (2009)

"The 2009 *NIS* represents several advances in the DNI's leadership of the NIP and the IC. It reflects a refined understanding of the counterterrorism challenge and elevates the importance of the challenges we face in the cyber domain and from counterintelligence threats. This *NIS* also affirms priorities to focus IC plans and actions for the next four years, while providing direction to guide development of future IC capabilities. The *NIS* highlights areas that demand our attention, resources, and commitment. It also establishes the basis for accountability, in conjunction with an implementation plan, to ensure that the Community meets the goals of our strategy."

- Dennis C. Blair, Former DNI, Forward to the *NIS*

The Mission Objectives detailed in the *NIS* are:

1. Combat violent extremism
2. Counter Weapons of Mass Destruction (WMD) proliferation

3. Provide strategic intelligence and warning
4. Integrate counterintelligence capabilities
5. Enhance cyber security
6. Support current operations (ongoing U.S. diplomatic, military, and law enforcement operations)

The Enterprise Objectives detailed in the NIS are:

1. Enhance community mission management
2. Strengthen partnerships
3. Streamline business processes
4. Improve information integration and sharing
5. Advance Science and Technology Research and Development (S&T/R&D)
6. Develop the workforce
7. Improve acquisition

Vision 2015

Vision 2015, a report prepared and released by the DNI on July 22, 2008, outlines the rationale for becoming an Intelligence Enterprise. It provides details on the differences between current and future operating models. *Vision 2015* states that the new Intelligence Enterprise will advance along the distinct paths of “adaptability, alignment, and agility.”

The U.S. intelligence system has evolved in the face of strategic and technological shifts throughout its history. Historically, the IC was siloed into distinct intelligence collection disciplines and functions, which led to competition between IC organizations and a duplication of effort. The agency-centric structure worked well during the Cold War, but it would not work in today’s rapidly changing environment.

Our world is a dynamic place where the pace, scope, and complexity of change is increasing. The key to achieving a lasting strategic advantage is the ability to rapidly and accurately anticipate and adapt to complex challenges. Intelligence must become more integrated and agile to assist in preventing and responding to new threats from non-traditional actors, new modes of attack, and the increasingly lethal impact of these attacks.

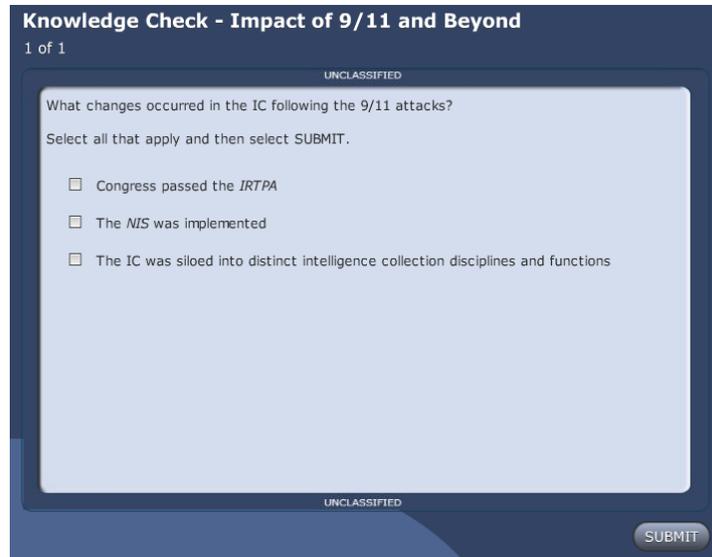
EO 12333 (2008)

Signed by President George W. Bush on July 31, 2008, *EO 12333* was amended to advance and institutionalize the reforms put into law by the *IRTPA* (2004) and to provide a framework for the conduct of our intelligence activities. It directs the community to produce timely, accurate, and insightful intelligence with special emphasis on international terrorism and the spread of weapons of mass destruction. In general, the amended EO does the following:

- Clarifies the responsibilities and strengthens the authority of the DNI
- Establishes policy on intelligence collection

NOTE: The EO banned assassinations and also states that human experimentation has limitations (retained from previous guidance)

- Defines the goal, direction, roles, and division of labor of each element in the IC
- Defines heads of elements of the IC and the CSA
- Maintains and strengthens protections for American civil liberties and privacy rights
- Strengthens protections of First Amendment rights of the U.S. Constitution
- Preserves and reinforces existing responsibilities of the IC members



Knowledge Check - Impact of 9/11 and Beyond

1. What changes occurred in the IC following the 9/11 attacks?

Select all that apply and then select SUBMIT.

Choice
Congress passed the <i>IRTPA</i>
The <i>NIS</i> was implemented
The IC was siloed into distinct intelligence collection disciplines and functions

The following table reflects the correct answers.

Correct	Choice
X	Congress passed the <i>IRTPA</i>
X	The <i>NIS</i> was implemented
	The IC was siloed into distinct intelligence collection disciplines and functions

Feedback when correct:

That's right! You selected the correct responses.

The correct answers are:

- Congress passed the *IRTPA*
- The *NIS* was implemented

The *IRTPA* significantly reformed the IC and intelligence-related activities of the U.S. Government. The *NIS* describes the drastic overhaul in the U.S. IC, including the implementation of a new system for sharing information and the integration of existing enterprises to meet mission objectives and enterprise objectives. The new focus of the IC is on global and changing threats.

The *Vision 2015* report explained that the agency-centric, or "siloed" structure historically donned by the IC worked well during the Cold War, but was inefficient in today's rapidly changing environment.

Feedback when incorrect:

You did not select the correct responses.

The correct answers are:

- Congress passed the *IRTPA*
- The *NIS* was implemented

The *IRTPA* significantly reformed the IC and intelligence-related activities of the U.S. Government. The *NIS* describes the drastic overhaul in the U.S. IC, including the implementation of a new system for sharing information and the integration of existing enterprises to meet mission objectives and enterprise objectives. The new focus of the IC is on global and changing threats.

The *Vision 2015* report explained that the agency-centric, or "siloed" structure historically donned by the IC worked well during the Cold War, but was inefficient in today's rapidly changing environment.

Summary

The events of WWII and 9/11 significantly changed the way the U.S. handles national security. Before WWII, our very simplistic national security methodology was focused on tactical intelligence. There was no global oversight for national intelligence and limited intelligence collection efforts existed.

WWII showed that this unsophisticated view of national security was grossly inadequate. After the surprise attack on Pearl Harbor, the OSS was established. Several secret programs, including Project ULTRA and the Manhattan Project, lead to new legislation and EOs. These governing documents introduced:

- The U.S. Government's SCI security system
- An integrated security program that included enhanced background checks of personnel and investigations of unauthorized disclosures
- A major reorganization of the U.S. Government's national security structure with the creation of the DoD and the Department of the Air Force
- Establishment of the IC
- Improvements to the quality of intelligence needed for national security
- Coordination of the intelligence departments and agencies

The events of 9/11 proved that terrorism had become a significant threat to the U.S. and its allies. The *9/11 Commission Report* findings strongly influenced the IC's change in methodology, leading to the creation or modification of legislation and EOs, the development of an IC-wide vision, the restructuring of the IC, and the development of the following documents:

- *IRTPA*
- *NIS*
- *Vision 2015*
- *EO 12333*

Summary

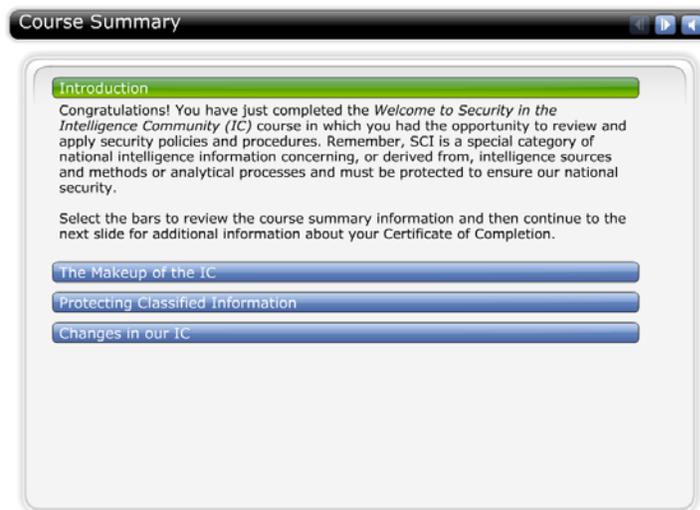
The events of WWII and 9/11 significantly changed the way the U.S. handles national security. Before WWII, our very simplistic national security methodology was focused on tactical intelligence. There was no global oversight for national intelligence and limited intelligence collection efforts existed.

WWII showed that this unsophisticated view of national security was grossly inadequate. After the surprise attack on Pearl Harbor, the OSS was established. Several secret programs, including Project ULTRA and the Manhattan Project, lead to new legislation and EOs. These governing documents introduced:

- The U.S. Government's SCI security system
- An integrated security program that included enhanced background checks of personnel and investigations of unauthorized disclosures
- A major reorganization of the U.S. Government's national security structure with the creation of the DoD and the Department of the Air Force
- Establishment of the IC
- Improvements to the quality of intelligence needed for national security
- Coordination of the intelligence departments and agencies

The events of 9/11 proved that terrorism had become a significant threat to the U.S. and its allies. The *9/11 Commission Report* findings strongly influenced the IC's change in methodology, leading to the creation or modification of legislation and EOs, the development of an IC-wide vision, the restructuring of the IC, and the development of the following documents:

- *IRTPA*
- *NIS*
- *Vision 2015*
- *EO 12333*



Course Summary

Introduction

Congratulations! You have just completed the *Welcome to Security in the Intelligence Community (IC)* course in which you had the opportunity to review and apply security policies and procedures. Remember, SCI is a special category of national intelligence information concerning, or derived from, intelligence sources and methods or analytical processes and must be protected to ensure our national security.

Select the bars to review the course summary information and then continue to the next slide for additional information about your Certificate of Completion.

The Makeup of the IC

The IC is led by the DNI and is comprised of 16 elements that fall into the Independent, DoD, and Departmental categories. The overall goal of the IC is to promote foreign relations and protect national intelligence information. The IC is also supported by non-NIP elements that help to “strengthen existing and establish new partnerships with foreign and domestic, public, and private entities to improve access to sources of information and intelligence, and ensure the appropriate dissemination of IC products and services.” The governing documents that define the IC are the *National Security Act*, the *IRTPA*, the *NIS*, and several EOs.

Protecting Classified Information

When you signed the Nda, you completed a life-long contract between yourself and the U.S. Government to protect national security information. Processes and procedures to which you agreed include PERSEC, physical and technical security, information assurance and cyber security, and classification management. You also agreed to additional requirements such as reporting unauthorized disclosures, submitting to pre-publication reviews, and reporting security incidents. Your SSO can answer any specific questions you have regarding your obligations.

Changes in our IC

The IC is constantly adapting based on lessons learned from events leading up to and during WWII and to 9/11. Since 9/11, threats against the U.S. and the IC have continued to evolve. Your knowledge of these threats and the resulting IC responses will help you to remain alert for new threats and adapt appropriately.



Welcome to Security in the IC
Certificate of Completion

Thank you. Now that you have completed the *Welcome to Security in the Intelligence Community (IC)* course, you need to print out your Certificate of Completion.

Select NEXT to Continue.

(Image Alt: ODNI logo)