

IC Security Today

Text Alternative



The Office of the Director of National Intelligence (ODNI)
Office of the National Counterintelligence Executive (ONCIX)
Special Security Directorate (SSD)
Community Services

Table of Contents

| | |
|--|-----|
| <i>IC Security Today</i> | 3 |
| <i>Lesson 1: Our Changing World</i> | 6 |
| Topic 1.1: Threats to Our National Security..... | 6 |
| Topic 1.2: The New Intelligence Community | 22 |
| Topic 1.3: SCI and the Key Security Methods..... | 50 |
| <i>Lesson 2: Scenario</i> | 109 |
| Course Summary..... | 129 |

Slide 1***IC Security Today***

(Image Alt: Title slide with ODNI seal)

Slide 2

Introduction

Welcome to your annual Sensitive Compartmented Information (SCI) refresher briefing. As a cleared professional, you are required to protect all classified information. SCI is a special category of National Security Information (NSI) 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 intelligence information. Throughout this course we will stress protection of SCI which safeguards intelligence information.

The Intelligence Community (IC) Security Today 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.

My name is Pat, and I will guide you through this training in order to reinforce your understanding and commitment to protect our nation's most sensitive classified information, SCI.

A small portrait of a man with grey hair, wearing a dark suit, a blue shirt, and a patterned tie. He is smiling slightly and looking towards the camera. The background of the portrait is dark with some American flag motifs.**Introduction**

Welcome to your annual Sensitive Compartmented Information (SCI) refresher briefing. As a cleared professional, you are required to protect all classified information. SCI is a special category of National Security Information (NSI) concerning, or derived from, intelligence sources and

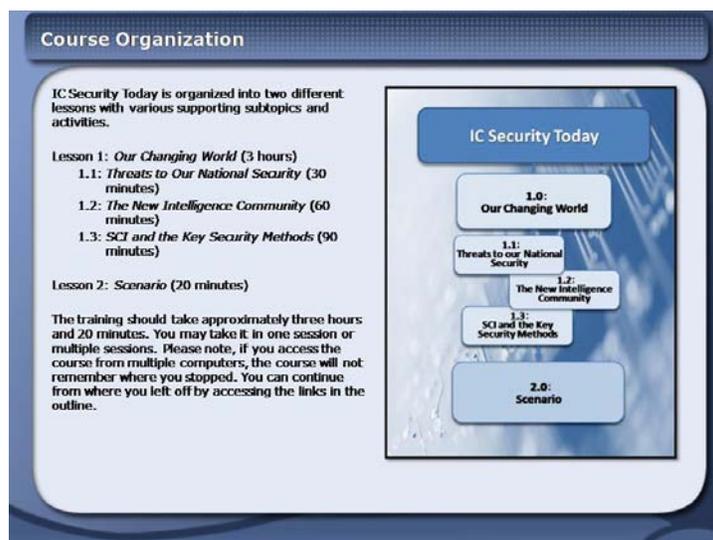
methods or analytical processes. Like other classified information, SCI must be protected to ensure our national security. As stated in *Intelligence Community Directive (ICD) 700*, the Director of National Intelligence (DNI) has established clear, uniform, and reciprocal SCI security policies and practices to protect this intelligence information. Throughout this course we will stress protection of SCI which safeguards intelligence information.

The Intelligence Community (IC) Security Today 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.

My name is Pat, and I will guide you through this training in order to reinforce your understanding and commitment to protect our nation's most sensitive classified information, SCI.

(Image Alt: Man, Pat, who will act as a guide while taking the course.)

Slide 3



Course Organization

IC Security Today is organized into two different lessons with various supporting subtopics and activities.

Lesson 1: *Our Changing World* (3 hours)

1.1: *Threats to Our National Security* (30 minutes)

1.2: *The New Intelligence Community* (60 minutes)

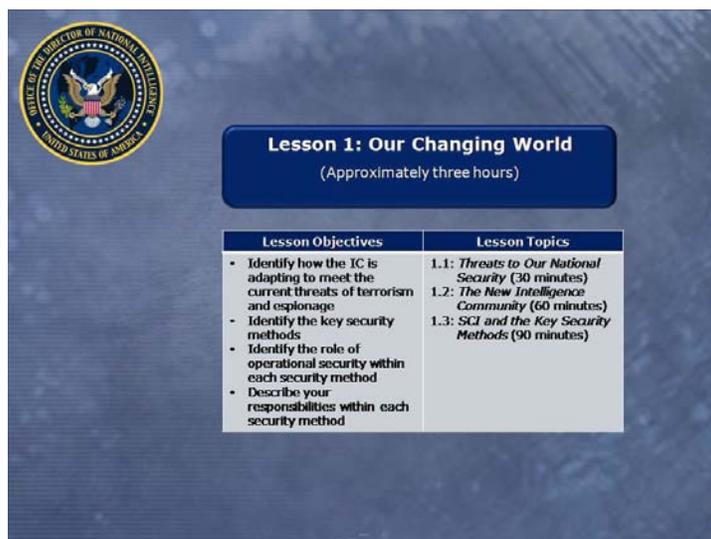
1.3: *SCI and the Key Security Methods* (90 minutes)

Lesson 2: *Scenario* (20 minutes)

The training should take approximately three hours and 20 minutes. You may take it in one session or multiple sessions. Please note, if you access the course from multiple computers, the course will not remember where you stopped. You can continue from where you left off by accessing the links in the outline.

(Image Alt: Course map listing the lesson and topic titles.)

Slide 4



| Lesson Objectives | Lesson Topics |
|---|---|
| <ul style="list-style-type: none">Identify how the IC is adapting to meet the current threats of terrorism and espionageIdentify the key security methodsIdentify the role of operational security within each security methodDescribe your responsibilities within each security method | <ul style="list-style-type: none">1.1: <i>Threats to Our National Security</i> (30 minutes)1.2: <i>The New Intelligence Community</i> (60 minutes)1.3: <i>SCI and the Key Security Methods</i> (90 minutes) |

Lesson 1: Our Changing World

(Approximately three hours)

Lesson Objectives

- Identify how the IC is adapting to meet the current threats of terrorism and espionage
- Identify the key security methods
- Identify the role of operational security within each security method
- Describe your responsibilities within each security method

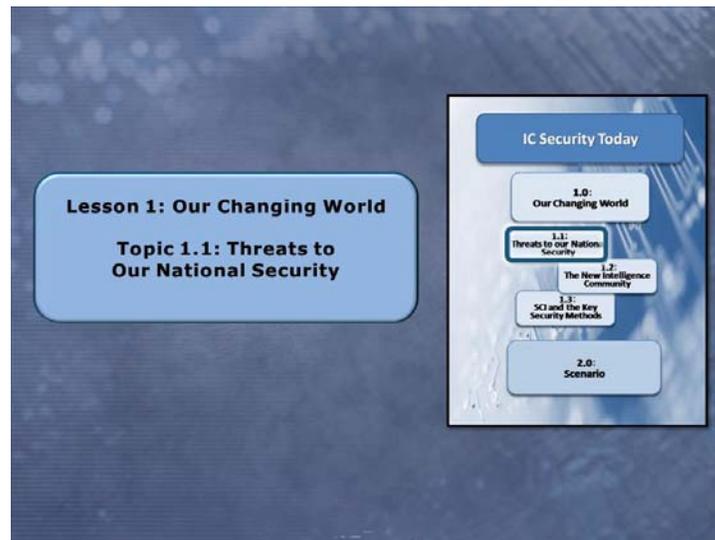
Lesson Topics

1.1: *Threats to Our National Security* (30 minutes)

1.2: *The New Intelligence Community* (60 minutes)

1.3: *SCI and the Key Security Methods* (90 minutes)

(Image Alt: Lesson title slide with ODNI seal.)

Slide 5**Lesson 1: Our Changing World****Topic 1.1: Threats to Our National Security**

(Image Alt: Course map highlighting Topic 1.1, *Threats to Our National Security*.)

Slide 6

Introduction and Objectives

As you know, threats to the United States (U.S.) have changed from those we faced in the last century. The biggest threat to our homeland is no longer the spread of communism; now there are different threats which come from different actors using different means.

We will spend some time exploring how the events of September 11, 2001 (9/11), and new and emerging threats, have changed the IC and our country as a whole.

Objectives

- Describe how the events of 9/11 have impacted the IC and led to a change in focus and business practices
- Describe how new tactics, technologies, and external factors are affecting persistent threats and creating new ones to our national security



Introduction and Objectives

As you know, threats to the United States (U.S.) have changed from those we faced in the last century. The biggest threat to our homeland is no longer the spread of communism; now there are different threats which come from different actors using different means.

We will spend some time exploring how the events of September 11, 2001 (9/11), and new and emerging threats, have changed the IC and our country as a whole.

Objectives

- Describe how the events of 9/11 have impacted the IC and led to a change in focus and business practices
- Describe how new tactics, technologies, and external factors are affecting persistent threats and creating new ones to our national security

(Image Alt: Pat standing in front of a collage containing images of various threats to national security. Some of these images include espionage, nuclear explosions, and terrorists.)

Slide 7

Determining Threats to National Security

Determining who, or what, is a threat to national security is not an easy task. Sometimes we determine that something is a threat only after we have been compromised or subjected to a catastrophic event (e.g., Pearl Harbor, 9/11). 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.

"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."

- National Intelligence Strategy (NIS), 2009



Determining Threats to National Security

Determining who, or what, is a threat to national security is not an easy task. Sometimes we determine that something is a threat only after we have been compromised or subjected to a catastrophic event (e.g., Pearl Harbor, 9/11). 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.

"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."

- National Intelligence Strategy (NIS), 2009

(Image Alt: Collage of terrorist carrying automatic weapons and an explosion.)

Slide 8

Pearl Harbor and 9/11

Let us take a look at two catastrophic events that occurred on U.S. soil that were both unprecedented and unforeseen. Pearl Harbor and the events of 9/11 changed society and the structure of our government agencies. They also led to dramatic changes in the IC. Both events defined and changed us.



| December 7, 1941 | September 11, 2001 |
|---|---|
| <p>The Japanese attacked Pearl Harbor. This surprise attack showed us that we were not immune from the war abroad and initiated U.S. entry into World War II (WWII). It also demonstrated that our government did not have a strategic intelligence capability.</p> | <p>Terrorists hijacked four U.S. planes and crashed, or attempted to crash them into U.S. buildings (two hit high-rise buildings, one hit the Pentagon, one crashed in Pennsylvania). These attacks not only showed us that we are vulnerable as a country, but also that we needed to improve our intelligence capabilities.</p> |
| <p>The attack sank four U.S. Navy battleships (two of which were later returned to service) and damaged four more. The Japanese also sank or damaged an additional seven ships and 188 aircraft and killed more than 2,400 people in the attack.</p> | <p>Approximately 3,000 people died in the terrorist attacks of 9/11, which were caused by "19 young Arabs acting at the behest of Islamist extremists headquartered in Afghanistan." (<i>The 9/11 Commission Report</i>)</p> |

Pearl Harbor and 9/11

Let us take a look at two catastrophic events that occurred on U.S. soil that were both unprecedented and unforeseen. Pearl Harbor and the events of 9/11 changed society and the structure of our government agencies. They also led to dramatic changes in the IC. Both events defined and changed us.

December 7, 1941

The Japanese attacked Pearl Harbor. This surprise attack showed us that we were not immune from the war abroad and initiated U.S. entry into World War II (WWII). It also demonstrated that our government did not have a strategic intelligence capability.

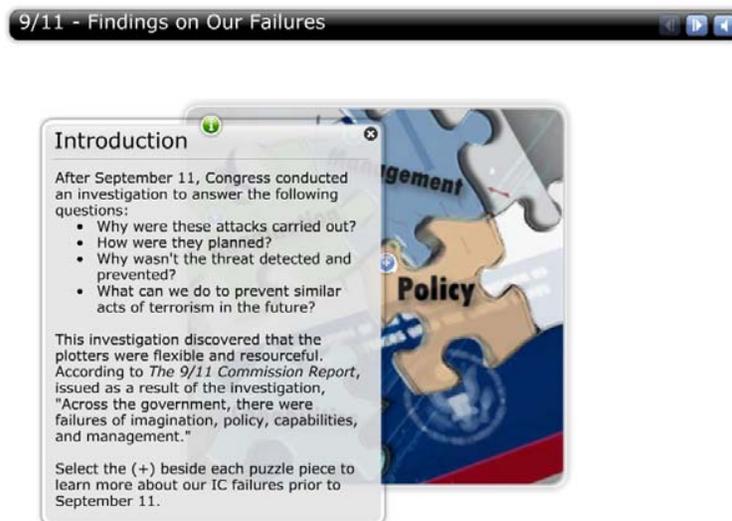
The attack sank four U.S. Navy battleships (two of which were later returned to service) and damaged four more. The Japanese also sank or damaged an additional seven ships and 188 aircraft and killed more than 2,400 people in the attack.

September 11, 2001

Terrorists hijacked four U.S. planes and crashed, or attempted to crash them into U.S. buildings (two hit high-rise buildings, one hit the Pentagon, one crashed in Pennsylvania). These attacks not only showed us that we are vulnerable as a country, but also that we needed to improve our intelligence capabilities. Approximately 3,000 people died in the terrorist attacks of 9/11, which were caused by "19 young Arabs acting at the behest of Islamist extremists headquartered in Afghanistan." (*The 9/11 Commission Report*)

(Image Alt: Collage showing the events of 9/11 and Pearl Harbor - for example, airplanes bombing aircraft carriers, crumbled World Trade Center Towers, man walking out of the debris covering his mouth.)

Slide 9



9/11 - Findings on Our Failures

(Interaction Alt: Roll over graphic containing five call-out boxes. Puzzle pieces detail four of the findings of the 9/11 Commission.)

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.

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.

Slide 10

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 | Government Organization |
|---|---|
| <p>This new global strategy sets out to dismantle the al Qaeda organization and prevail over the ideology that contributes to Islamist extremists.</p> <p>The strategy has three components:</p> <ol style="list-style-type: none"> 1. Attack terrorists and their organizations 2. Prevent the continued growth of Islamist terrorism 3. Prepare for, and protect against, terrorist attacks <p>NOTE: This strategy, as it pertains to you, will include improving information sharing and curbing unauthorized disclosures.</p> | <p>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,</p> <p style="text-align: center;"><i>"Build a unity of effort across the U.S. Government."</i></p> <p style="text-align: right;"><i>–The 9/11 Commission Report</i></p> <p>Revisions to the government included:</p> <ol style="list-style-type: none"> 1. Creating a National Counterterrorism Center (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 Federal Bureau of Investigation (FBI) and homeland defenders |

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 a National Counterterrorism Center (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 Federal Bureau of Investigation (FBI) and homeland defenders

Slide 11

9/11 – Implications for National 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 Executive Orders (EO), the development of an IC-wide vision, and a restructuring of the IC.



9/11 – Implications for National 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 Executive Orders (EO), the development of an IC-wide vision, and a restructuring of the IC.

(Image Alt: Collage of potential threats: computer networks, files, lock door and an explosion.)

Slide 12



Expanding Threat Matrix - Global Forces

(Interaction Alt: Rollover interaction illustrating the various global forces expanding the threat matrix.)

Introduction

Vision 2015, signed July 2, 2008, explores the forces that are leading the U.S. to change its strategic landscape. These forces are "colliding," "reinforcing," "amplifying," and "reshaping" our strategic landscape.

Because we work with NSI, we need to be aware of these factors and the opportunities and risks that they represent.

Select each of the global forces (+) to see examples of the opportunities and risks associated with them.

For more information on *Vision 2015*, access the attachments tab.

Political & Military

(Image Alt: Soldiers with machine guns and artillery)

Opportunity

Democracy

Risk

State Instability

Innovation & Technology

(Image Alt: Brain)

Opportunity

Scientific Advancement

Risk

Proliferation

Economic & Financial

(Image Alt: Currency)

Opportunity

Economic Growth

Risk

Growing Disparity in Income Levels

Demographic

(Image Alt: People)

Opportunity

Changing Workforce Demographics

Risk

Stressed Pension Systems

Social & Cultural

(Image Alt: Globe with hands supporting it)

Opportunity

Urbanization

Risk

Social Dislocation

Energy & Environment

(Image Alt: Windmills)

Opportunity

Affordable Energy

Risk

Environmental Degradation

Current Events

The popular uprisings in countries such as Egypt, Tunisia, Morocco and Libya; the tsunami and nuclear disaster in Japan; and the continued concern with nuclear proliferation are example of these new threats to national security.

Slide 13



Expanding Threat Matrix – Persistent and Emerging Threats

Just because the world is changing does not mean that we have solved the problems of the past. Those problems and their associated threats are still alive and we must strive to make sure that they do not turn into reality.

We need to continue to live in the present and defend ourselves against persistent threats.

We also need to prepare for the future and look at emerging threats and how they affect our future missions.

As members of the IC, we must prepare for, and defend ourselves against, all of these threats, whether they are from the past, persistent, or emerging.

(Image Alt: Globe surrounded by images showing persistent and emerging threats. These include Failed States, Weapons of Mass Destruction, Cyber, Economic, Space, Energy, Climate Change, Rogue States, Insurgencies, Terrorism, Crime/Gangs, and Drugs.)

Slide 14

Expanding Threat Matrix – Cyber and Digital Threats

Cyber and digital threats are two important threats of which to be aware. Most people know that cyber criminals and hackers use viruses and Trojan horses to destroy our computers. But traditional and cyber terrorists, as well as nations, are using computers and the Internet to further their interests.

For example, traditional terrorists are using the Internet to:

- Recruit and communicate with members of their organizations
- Coordinate terrorist activities with other aligned groups
- Raise money through cyber crime
- Perform propaganda

Cyber terrorists from thousands of miles away are looking to bring down the national information infrastructures of countries they deem hostile. The consequences of a cyber attack like this could be catastrophic.

Distributed Denial of Service Attack
July 2008 - More than 35 government websites in the U.S. and S. Korea were attacked.

Distributed Denial of Service Attack
August 2009 - Twitter crashed when attackers were trying to stop a lone blogger in "Cyxmyu," a city in Georgia. It is suspected that the attack was related to political conflict between two countries.

Attack on Critical Infrastructure
April 2009 - The U.S. electrical grid was penetrated by foreign cyber spies. It is suspected that the spies were from several other countries. They penetrated the system's vulnerabilities and left behind potentially dangerous software.

Attack Using Viruses
April 2008 - The Pentagon's networks were attacked by a global worm or virus. This caused the military to temporarily ban the use of removable media.

Google Email Hacked
January 2010 - Google Gmail was hacked and anti-government users.

Expanding Threat Matrix – Cyber and Digital Threats

Cyber and digital threats are two important threats of which to be aware. Most people know that cyber criminals and hackers use viruses and Trojan horses to destroy our computers. But traditional and cyber terrorists, as well as nations, are using computers and the Internet to further their interests.

For example, traditional terrorists are using the Internet to:

- Recruit and communicate with members of their organizations
- Coordinate terrorist activities with other aligned groups
- Raise money through cyber crime
- Perform propaganda

Cyber terrorists from thousands of miles away are looking to bring down the national information infrastructures of countries they deem hostile. The consequences of a cyber attack like this could be catastrophic.

Examples:

Distributed Denial of Service Attack

July 2008 - More than 35 government websites in the U.S. and S. Korea were attacked.

Distributed Denial of Service Attack

August 2009 - Twitter crashed when attackers were trying to stop a lone blogger in "Cyxmyu," a city in Georgia. It is suspected that the attack was related to political conflict between two countries.

Attack on Critical Infrastructure

April 2009 – The U.S. electrical grid was penetrated by foreign cyber spies. It is suspected that the spies were from several other countries. They penetrated the system's vulnerabilities and left behind potentially dangerous software.

Attack Using Viruses

April 2008 - The Pentagon's networks were attacked by a global worm or virus. This caused the military to temporarily ban the use of removable media.

Google Email Hacked

January 2010- Google Gmail was hacked and compromised in China. Hackers focused on antigovernment users.

Slide 15

The events of 9/11 showed the IC that its current business practices were not enough to protect the U.S. The 9/11 Commission made recommendations for how the IC needed to change.

Review the following recommendations, select all that were made by the 9/11 Commission, and then select SUBMIT.

- Develop a global strategy against terrorism
- Reorganize the national security institutions to be more enterprise focused
- Be more imaginative as to the threats to national security
- Maintain the current organization and mission of each agency within the IC
- All of the above



Impact of 9/11 on the IC

1. The events of 9/11 showed the IC that its current business practices were not enough to protect the U.S. The 9/11 Commission made recommendations for how the IC needed to change.

Review the following recommendations, select all that were made by the 9/11 Commission, and then select SUBMIT.

| Correct | Choice |
|---------|---|
| X | Develop a global strategy against terrorism |
| X | Reorganize the national security institutions to be more enterprise focused |
| | Be more imaginative as to the threats to national security |

| |
|--|
| Maintain the current organization and mission of each agency within the IC |
|--|

| |
|------------------|
| All of the above |
|------------------|

Feedback when correct:

That's right! You selected the correct responses.

The 9/11 Commission recommended that the IC:

- Develop a global strategy against terrorism
- Reorganize the national security institutions to be more enterprise-focused

Being more imaginative as to the threats to national security is incorrect. Lack of imagination was one of the IC's failures prior to 9/11. However, being more imaginative does not mean that the IC can gather information on terrorism and other threats to national security by any means necessary. There are policies and parameters about on whom we can gather intelligence and by what means it can be gathered.

Maintain the current organization and mission of each agency within the IC is incorrect because the 9/11 Commission recommended a reorganization of national security institutions.

Feedback when incorrect:

You did not select the correct response.

The 9/11 Commission recommended that the IC:

- Develop a global strategy against terrorism
- Reorganize the national security institutions to be more enterprise-focused

Being more imaginative as to the threats to national security is incorrect. Lack of imagination was one of the IC's failures prior to 9/11. However, being more imaginative does not mean that the IC can gather information on terrorism and other threats to national security by any means necessary. There are policies and parameters about on whom we can gather intelligence and by what means it can be gathered.

Maintain the current organization and mission of each agency within the IC is incorrect because the 9/11 Commission recommended a reorganization of national security institutions.

(Image Alt: Image of the New York Times 9/11 attack.)

Slide 16

Summary

The threats of the 21st Century are not the same as those in the 20th Century. The government has identified organizational shortcomings and new threats affecting national security. As a result, the IC is positioning itself to better anticipate, respond to, and mitigate emerging threats. For example:

- The 9/11 Commission identified IC failures and called for a change in our global strategy and organization
- *Vision 2015* described how the IC needs to expand its threat matrix to identify persistent and emerging threats based on new tactics and technologies, and also on external factors, so that we can respond to them appropriately

As a cleared professional, it is important that you are aware of the persistent and emerging threats affecting our national security. It is also important to understand how the IC is changing to respond to these threats. In the next section, we will discuss how the IC is becoming more adaptive, agile, and integrated.



Summary

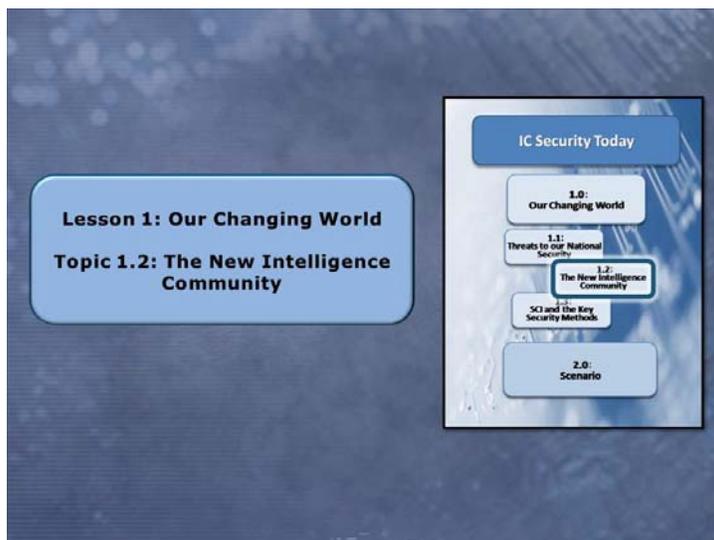
The threats of the 21st Century are not the same as those in the 20th Century. The government has identified organizational shortcomings and new threats affecting national security. As a result, the IC is positioning itself to better anticipate, respond to, and mitigate emerging threats. For example:

- The 9/11 Commission identified IC failures and called for a change in our global strategy and organization
- *Vision 2015* described how the IC needs to expand its threat matrix to identify persistent and emerging threats based on new tactics and technologies, and also on external factors, so that we can respond to them appropriately

As a cleared professional, it is important that you are aware of the persistent and emerging threats affecting our national security. It is also important to understand how the IC is changing to respond to these threats. In the next section, we will discuss how the IC is becoming more adaptive, agile, and integrated.

(Image Alt: Pat in front of a collage of threats that affect (i.e., terrorists) and events (i.e., 9/11) that have affected our national security.)

Slide 17



Lesson 1: Our Changing World

Topic 1.2: The New Intelligence Community

(Image Alt: Course map highlighting Topic 1.2, *The New Intelligence Community*.)

Slide 18

Introduction and Objectives

The continuing threats to our homeland and the emerging missions of the IC have shown us that the IC's old culture and structure could not sufficiently protect our country. This has led to major changes in the IC. Inter- and intra-agency collaboration is being encouraged both inside and outside of the IC. Intelligence is being gathered from new sources and a new level of oversight has been incorporated. The IC is changing to become a single enterprise that is more agile, adaptive, and responsive.

We will spend the next few minutes exploring the IC, its components and their missions, the Office of the Director of National Intelligence (ODNI) and its role in security, and the governing documents that are the foundation for the IC.

Objectives

- Identify the new structure of the IC
- Identify the key governing documents that define the IC and the capabilities of each IC element
- Identify the DNI's role in security planning, policy, and execution
- Describe the actions that the DNI is taking to improve and standardize security policies and procedures across the IC

Introduction and Objectives

The continuing threats to our homeland and the emerging missions of the IC have shown us that the IC's old culture and structure could not sufficiently protect our country. This has led to major changes in the IC. Inter- and

intra-agency collaboration is being encouraged both inside and outside of the IC. Intelligence is being gathered from new sources and a new level of oversight has been incorporated. The IC is changing to become a single enterprise that is more agile, adaptive, and responsive.

We will spend the next few minutes exploring the IC, its components and their missions, the Office of the Director of National Intelligence (ODNI) and its role in security, and the governing documents that are the foundation for the IC.

Objectives

- Identify the new structure of the IC
- Identify the key governing documents that define the IC and the capabilities of each IC element
- Identify the DNI's role in security planning, policy, and execution
- Describe actions that the DNI is taking to improve and standardize security policies and procedures across the IC

(Image Alt: Pat in front of a collage of images representing the IC members and their capabilities (i.e., agency seals, leaders, and satellites, etc.)

Slide 19

Definition of the Intelligence Community

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 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



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

Definition of the Intelligence Community

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 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

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

(Image Alt: ODNI seal surrounded by images of the U.S. agencies.)

Slide 20

The screenshot shows a presentation slide with a title bar that reads "Governing Documents that Define the IC". The slide content is as follows:

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.

At the bottom of the slide is a horizontal timeline with four colored segments: purple (1940-1969), blue (1970-1979), green (1980-1999), and light blue (2000-2010). Each segment has a small circle icon above it.

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 *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
- Central Intelligence Agency (CIA)

It merged the War and Navy Departments into a single Department of Defense (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 WWII era, and also out of small, post-war, intelligence organizations. It served as the primary civilian, intelligence-gathering entity. Later, the Defense Intelligence Agency (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:
 1. Military services
 2. FBI
 3. Department of State (DOS)
 4. Department of the Treasury
 5. 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 *Intelligence Reform and Terrorism Prevention Act (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:

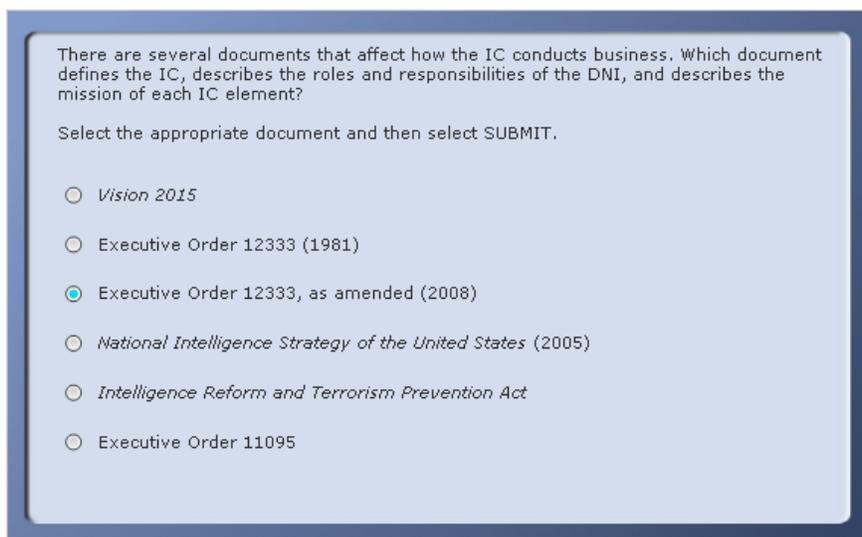
- Lays out the strategic environment - challenges we face from other nations and non-state actors and those from global trends related to forces (i.e., economic, environmental, technological, pandemic)
- Describes mission and enterprise objectives
- Sets priorities and objectives
- Guides current and 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

E.O. 13549: Classified National Security Program for SLTP (2010)

E.O. 13549, "Classified National Security Program for State, Local, Tribal & Private Entities" of August 18 2010, established a program designed to safeguard and govern access to classified national security information shared by the Federal Government with State, Local, Tribal & Private (SLTP) entities to further the information-sharing responsibilities set forth in the IRTPA.

Slide 21



Governing Documents

1. There are several documents that affect how the IC conducts business. Which document defines the IC, describes the roles and responsibilities of the DNI, and describes the mission of each IC element?

Select the appropriate document and then select SUBMIT.

| Correct | Choice | Feedback |
|---------|--------------------|--|
| | <i>Vision 2015</i> | You did not select the correct response. <i>Vision 2015</i> outlines a way forward for the IC to achieve a globally-networked and integrated intelligence enterprise for the 21st century. |

| | | |
|---|--|---|
| | | <p>The correct answer is <i>EO 12333</i>, as amended (2008). This order defines the IC, describes the roles and responsibilities of the DNI, and describes the mission of each element.</p> |
| | <p><i>Executive Order 12333 (1981)</i></p> | <p>You did not select the correct response. <i>EO 12333 (1981)</i> established the IC and defined the roles and responsibilities of U.S. departments and agencies. However, the Office of the DNI was not established until 2004 when the <i>IRTPA</i> was signed into law.</p> <p>The correct answer is <i>EO 12333</i>, as amended (2008). This order defines the IC, describes the roles and responsibilities of the DNI, and describes the mission of each element.</p> |
| X | <p><i>Executive Order 12333, as amended (2008)</i></p> | <p>You selected the correct response. <i>EO 12333</i> as amended in 2008 defines the IC, describes the roles and responsibilities of the DNI, and describes the mission of each element.</p> |
| | <p><i>National Intelligence Strategy of the United States (2005)</i></p> | <p>You did not select the correct response. <i>The National Intelligence Strategy</i> provides our approach (a blueprint) for how the IC will operate.</p> <p>The correct answer is <i>EO 12333</i>, as amended (2008). This order defines the IC, describes the roles and responsibilities of the DNI, and describes the mission of each element.</p> |
| | <p><i>Intelligence Reform and Terrorism Prevention Act</i></p> | <p>You did not select the correct response. <i>IRTPA</i> was designed to reform the IC and the intelligence and intelligence-related activities of the U.S. Government, and for other purposes.</p> <p>The correct answer is <i>EO 12333</i>, as amended (2008). This order defines the IC, describes the roles and</p> |

| | |
|-------------------------------------|---|
| | <p>responsibilities of the DNI, and describes the mission of each element.</p> |
| <p><i>Executive Order 11095</i></p> | <p>You did not select the correct response. <i>EO 11905</i> established 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.</p> <p>The correct answer is <i>EO 12333</i>, as amended (2008). This order defines the IC, describes the roles and responsibilities of the DNI, and describes the mission of each element.</p> |

Slide 22



Members of the IC

(Interaction Alt: Roll over interaction illustrating organization of the Intelligence Community using agency seals.)

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 roles 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*.

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 Homeland Security Council (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.

Slide 23

Other Partners

The intelligence activities of the U.S. expand beyond these 16 elements of the IC. One of the enterprise objectives of the *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-National Intelligence Program (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 *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-National Intelligence Program (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.

Pop Up: Non-Title 50 Organizations

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 (NASA)

(Image Alt: Man and woman shaking hands at a National Intelligence conference surrounded with images of IC product and services.)

Slide 24



IC Functional Managers

(Interaction Alt: Roll over of the seals of the six agencies that are functional managers – CIA, NSA, NRO, NGA, and FBI)

Introduction

As you can see the IC has grown in size and capabilities. It has six functional managers responsible for the management and oversight of various programs. Five of these functional managers come from agencies whose only responsibility is intelligence.

Select the (+) next to the seals to learn each agency's area of responsibility.

CIA

The Director of the CIA is the functional manager of:

- The National Clandestine Service (NCS)

- The Human Intelligence (HUMINT) Control System Manual

NSA

The Director of NSA Consolidated Security Service (CSS) is the functional manager of:

- The SIGINT Program
- SIGINT Security Regulations

NRO

The Director of the NRO is the functional manager of:

- The National Reconnaissance Program
- The RESERVE Control System Manual

NGA

The Director of the NGA is the functional manager of:

- Geospatial Intelligence (GEOINT)
- The Imagery Policy Series
- The KLONDIKE Control System

FBI

The FBI Executive Assistant Director for the NSB is the functional manager of:

- Counterterrorism
- Counterintelligence
- Domestic intelligence in support of the above

NOTE: The FBI has responsibilities outside of the NIP.

DIA

The Director of the DIA is the functional manager of:

- The General Defense Intelligence Program (GDIP)
- Measurement and Signature Intelligence (MASINT)
- The MASINT Policy Series

Slide 25

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)



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.

| 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.

Slide 26**Role of the Director of National Intelligence (DNI)**

The IC is lead by the DNI. The ODNI was established in 2005 after the creation of the *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 HSC and also oversees and directs the implementation of the NIP.

(Image Alt: Official pictures of the four past DNI's.)

Slide 27

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.



```
graph TD; A[We the People  
Authority] --> B[Congress]; A --> C[President]; B --> D[Executive Orders  
Presidential Policy Directives]; C --> D; D --> E[ICD Policies];
```

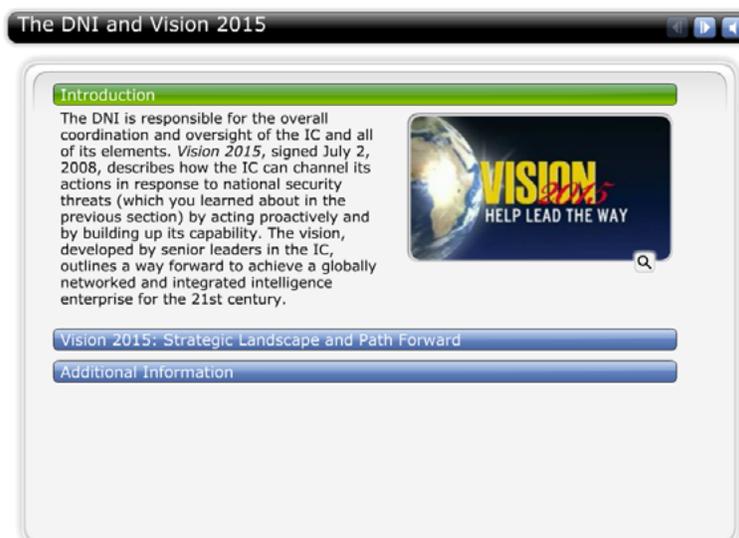
Policy Development

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 showing how policy is developed. Starts with the Constitution and the authority it grants, then either Congress uses its authority to create laws or the President uses his authority to create Executive Orders and Presidential Policy Directives, these then go to the DNI for interpretation and are released in the form of policies and procedures.)

Slide 28



The DNI and Vision 2015

(Interaction Alt: Question interaction with embedded video)

Introduction

The DNI is responsible for the overall coordination and oversight of the IC and all of its elements. *Vision 2015*, signed July 2, 2008, describes how the IC can channel its actions in response to national security threats (which you learned about in the previous section) by acting proactively and by building up its capability. The vision, developed by senior leaders in the IC, outlines a way forward to achieve a globally networked and integrated intelligence enterprise for the 21st century.

Vision 2015: Strategic Landscape and Path Forward

A text alternative can be found under the Attachments tab.

6 minutes 15 seconds video. The transcript is below.

Vision 2015: Strategic Landscape and Path Forward

Text Alternative for the Video

Vision 2015, a globally networked and integrated Intelligence Enterprise. We live in a dynamic world in which the pace, scope, and complexity of change are increasing. Isolated forces and events are now increasingly connected: innovation and technology, energy and environment, political and military, social and cultural, demographic and health, and economic and financial. These forces are intersecting, reinforcing, and amplifying to produce a complex and unpredictable risk environment and a less predictable future. In

such a future, anticipating and avoiding strategic surprise grows in importance.

The implication for our national security community is that the combination of speed, complexity, and unpredictability in this environment blur traditional distinctions, definitions, and boundaries undermining existing organizational constructs and operating models. These include traditional national security missions versus non-traditional missions, foreign versus domestic, customers versus producers, strategic versus tactical, collection versus analysis, open versus secret, intelligence versus information, and off-the-shelf technology versus proprietary technology. The challenge to our Intelligence Community is to achieve expanded awareness of events and trends on a global scale and quickly develop deep insights on critical issues when needed while considering alternative hypotheses, scenarios, and outcomes, and determining linkages and possibilities among a range of complex issues.

With the right combination of global awareness, deep insight, and strategic foresight, we will accomplish our intelligence mission: create decision advantage for our customers. Decision advantage means we collect and analyze intelligence to improve our customer's ability to make a decision while denying our adversaries the same advantage (e.g., chess moves and countermoves to block opponents). As the world has evolved, so must we evolve. To compete against networked threats, we must become networked ourselves. The key question is, "How do we create a globally networked intelligence enterprise?"

Decision Advantage: Enterprise Integration, Net-centric Information Enterprise, Mission-Focused Operations, and Customer Driven Intelligence

First, we must create a collaborative foundation to build on. We must share information across organizational boundaries. We must ensure unity of effort on shared missions in order to provide the customer the right information, at the right time, in the right format.

By 2015 we will be expected to provide more details about more issues to more customers (i.e., customer-driven intelligence: what's going on and what does it mean). This means supporting a broader range of customers, establishing deeper relationships to ensure greater relevance, and responding with tailored products and services to customers accustomed to on-demand information (i.e., customer-driven intelligence: what's next and who knows more).

All this requires that we change our current operating model and move from an agency-centric to a mission-focused model where capabilities and expertise can be rapidly assembled and orchestrated around a shared mission.

Integrated Mission Management, Adaptive Collection, Collaborative Analytics, and Strategic Partnerships

This focus will allow us to link diverse expertise and resources against specific missions, dynamically reallocate collection and analytic assets in response to rapidly unfolding events, and collaboratively exploit and share vast stores of information in real time. Key to all of this is a foundation built on strategic partnerships with state and local governments, our allies, foreign partners, academia, and the private sectors to improve global coverage and information sharing.

To enable such operations we must field an information-sharing platform that will provide on-demand access, discovery, exploitation, and sharing. This net-centric information enterprise will ensure that intelligence producers and customers have the right access to the right information at the right time. However, none of this can happen without a collaborative foundation.

Culture; Business Practices; Innovation, Science, and Technology; Facilities and Logistics; Human Capital; and Policy

This means providing educational initiatives to further our workforce through programs like Joint Duty and the National Intelligence University; reforming the security clearance process and modernizing our procurement and acquisition processes making them more agile and responsive to change; harnessing America's technology edge to out-manuever our adversaries; investing in our facilities to ensure greater utilization of scarce resources; standardizing our pay and performance systems across the enterprise; and developing a strong policy foundation to grow with in the future.

So, how can we make that happen (i.e., nice vision, but get real). To translate our vision into reality, we need to understand and address the institutional and cultural barriers to change. [Some concerns include: With what money? I don't understand. What's my incentive? What's in it for me?] First, the vision must be made clear and communicated to the workforce. It must be placed on the management agenda and be supported by leadership at all levels. Resources and investments must be allocated to accomplish the vision. The incentives and accountability must be clearly aligned towards realizing the vision.

Achieving this vision will take personal engagement and leadership at all levels of every agency. So ask yourself:

- Where do I fit in?
- What can I do?
- What action can I take today to change tomorrow?

Remember:

- The Vision – A globally networked and integrated intelligence enterprise
- The Mission – Creating decision advantage

Take a step. Help lead the way.

Video Source: <https://www.intelink.gov/ivideo/default.aspx?id=30A4306B-6514-4678-85FC-5A85F5B812F8>

Additional Information

Additional information about *Vision 2015* can be found on Intelink and from the Attachments tab of this course.

- *Vision 2015* on Intelink web site (unclassified)
<https://www.intelink.gov/sites/vision2015/home/default.aspx>
- *Vision 2015* (pdf)
- *Vision 2015* Video Text Alternative

Slide 29

Role of DNI in Security

As the person in charge of managing the IC, the DNI plays various, important roles. Several of the challenges the DNI faces are security focused:

- Protecting intelligence sources and methods
- Promoting uniform security policies and procedures
- Acting as the Executive Agent for all security clearances in the U.S. Government
- Leading government-wide security clearance reform - with the intention of streamlining and standardizing processes and requirements such as:
 - Standardizing reciprocity for security clearances across agencies
 - Streamlining the process to shorten the length of time for the investigation and adjudication of security clearances

"Nothing is more important to national security than the making and the conduct of good security policies and timely, accurate, objective and relevant intelligence."

Dennis C. Blair,
Former DNI

Role of DNI in Security

As the person in charge of managing the IC, the DNI plays various important roles. Several of the challenges the DNI faces are security focused:

- Protecting intelligence sources and methods
- Promoting uniform security policies and procedures

- Acting as the Executive Agent for all security clearances in the U.S. Government
 - Leading government-wide security clearance reform - with the intention of streamlining and standardizing processes and requirements such as:
 - Standardizing reciprocity for security clearances across agencies
 - Streamlining the process to shorten the length of time for the investigation and adjudication of security clearances

“Nothing is more important to national security than the making and the conduct of good security policies and timely, accurate, objective and relevant intelligence.”

- Dennis C. Blair, Former DNI

Slide 30

DNI Security Initiatives – Security Clearance Investigations

In the past, the Government has been criticized for having an unresponsive security clearance process.

IRTPA (2004) now requires that 90% of initial security clearance processes for new government hires and contractors are to be completed within 60 days of submission date.

- 40 days on average for investigations
- 20 days on average for adjudications

To meet Congressional mandates, the Security and Suitability Process Reform has been implemented by the Director of the Office of Management and Budget (OMB). Under this initiative, the DNI will serve as the Security Executive Agent.

NOTE: This DNI's authority as the Security Executive Agent is established in FO 13467, *Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (July 2008).

How Are We Doing?

Average Days to Process a Security Clearance

| Year | Top Secret (Days) | Initial Secret Clearance (Days) |
|------------|-------------------|---------------------------------|
| 2005 | ~350 | ~250 |
| Sept. 2009 | ~100 | ~150 |

Backlog of pending security clearance investigations:

- 2006 - almost 100,000 cases
- September 2009 - none

Source: Security Clearance Reform: Moving Forward on Modernization Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia (15 September 2009)

DNI Security Initiatives – Security Clearance Investigations

In the past, the Government has been criticized for having an unresponsive security clearance process.

IRTPA (2004) now requires that 90% of initial security clearance processes for new government hires and contractors are to be completed within 60 days of submission date.

- 40 days on average for investigations
- 20 days on average for adjudications

To meet Congressional mandates, the Security and Suitability Process Reform has been implemented by the Director of the Office of Management

and Budget (D/OMB). Under this initiative, the DNI will serve as the Security Executive Agent.

NOTE: This DNI's authority as the Security Executive Agent is established in *EO 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information* (July 2008).

(Image Alt: Graph showing the average number of days to process a security clearance.)

Slide 31



DNI's Role in Security

1. The DNI's role in security reform includes the following tasks:
 - Promoting intelligence knowledge sharing
 - Protecting intelligence sources and methods
 - Promoting uniform procedures for SCI
 - Acting as the Executive Agent for all security clearances in the U.S. Government

Select the appropriate response and then select SUBMIT.

| Correct | Choice |
|---------|--------|
| X | True |
| | False |

Feedback when correct:

You selected the correct response.

The DNI's role in security is focused on promoting knowledge sharing, protecting sources and methods, promoting uniform procedures, and improving the security clearance process.

Feedback when incorrect:

You did not select the correct response.

The DNI's role in security is focused on promoting knowledge sharing, protecting sources and methods, promoting uniform procedures, and improving the security clearance process.

(Image Alt: Graph showing the ODNl emblem.)

Slide 32

Summary

Most Americans would agree that recent events in our history have identified flaws in our intelligence and government organizations. Various Presidential orders and Congressional mandates have changed the way we do business in order to make us more adaptive, agile, and integrated. These changes include:

- Restructuring the IC to include a DNI and new members
- Defining and clarifying responsibilities of various IC elements
- Defining each IC element's mission and capabilities
- Redefining how the IC collects intelligence
- Streamlining and standardizing security policies and procedures
- Improving the security clearance process
- Encouraging collaboration with other organizations both within and outside of the IC

The DNI is charged with managing the IC and changes within it. As a cleared national intelligence professional, you are tasked with following these regulations and promoting these initiatives.

Summary

Most Americans would agree that recent events in our history have identified flaws in our intelligence and government organizations. Various Presidential orders and Congressional mandates have changed the way we do business in order to make us more adaptive, agile, and integrated. These changes include:

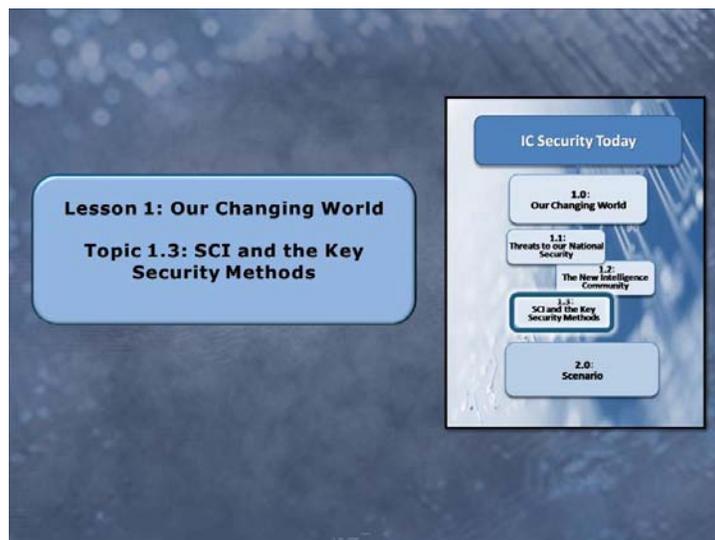
- Restructuring the IC to include a DNI and new members
- Defining and clarifying responsibilities of various IC elements
- Defining each IC element's mission and capabilities
- Redefining how the IC collects intelligence
- Streamlining and standardizing security policies and procedures
- Improving the security clearance process

- Encouraging collaboration with other organizations both within and outside of the IC

The DNI is charged with managing the IC and changes within it. As a cleared national intelligence professional, you are tasked with following these regulations and promoting these initiatives.

(Image Alt: Collage of people standing in front of an American flag.)

Page 33



Lesson 1: Our Changing World

Topic 1.3: SCI and the Key Security Methods

(Image Alt: Course map highlighting Topic 1.3, *SCI and the Key Security Methods*.)

Slide 34

Introduction

As we have learned, there are persistent and emerging threats that are changing the U.S. strategic landscape. We also learned how certain events in history have changed the government and the IC both structurally and culturally. The IC is learning from these events and preparing for the future. We will continue to strive to make the IC more agile, adaptive, and integrated to give our government the decision advantage.

While there have been many changes in the IC, there are some things that remain the same; the key security methods and our need to protect SCI. There are four key security methods:

1. Personnel Security
2. Physical and Technical Security
3. Information Assurance and Cyber Security
4. Classification Management

As cleared professionals, it is our duty to continue to serve our country by protecting its most sensitive information. This includes the use of *Operations Security (OPSEC)* measures in support of each method. This section of the briefing will remind you of the security policies and your responsibilities in each of the four major security methods.

Introduction

As we have learned, there are persistent and emerging threats that are changing the U.S. strategic landscape. We also learned how certain events in history have changed the government and the IC both structurally and

culturally. The IC is learning from these events and preparing for the future. We will continue to strive to make the IC more agile, adaptive, and integrated to give our government the decision advantage.

While there have been many changes in the IC, there are some things that remain the same; the key security methods and our need to protect SCI. There are four key security methods:

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

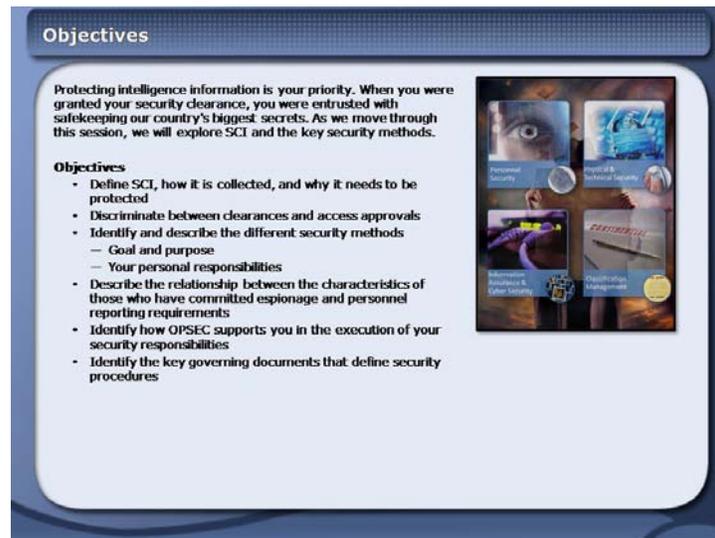
As cleared professionals, it is our duty to continue to serve our country by protecting its most sensitive information. This includes the use of [Operations Security \(OPSEC\)](#) measures in support of each method. This section of the briefing will remind you of the security policies and your responsibilities in each of the four major security methods.

Pop Up: Operations Security (OPSEC)

The process of denying potential adversaries any information about capabilities and/or intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities.

(Image Alt: Four images representing each of the key security disciplines: Fingerprints and retinal scans representing Personnel Security; a key board with a lock and a safe spin dial representing Physical Security, a router and computer monitors representing Information Assurance and Cyber Security, and a Confidential folder and a document t marked TOP SECRET representing Classification Management. NOTE: This image is used throughout this topic.)

Slide 35



Objectives

Protecting intelligence information is your priority. When you were granted your security clearance, you were entrusted with safekeeping our country's biggest secrets. As we move through this session, we will explore SCI and the key security methods.

Objectives

- Define SCI, how it is collected, and why it needs to be protected
- Discriminate between clearances and access approvals
- Identify and describe the different security methods
 - Goal and purpose
 - Your personal responsibilities
- Describe the relationship between the characteristics of those who have committed espionage and personnel reporting requirements
- Identify how OPSEC supports you in the execution of your security responsibilities
- Identify the key governing documents that define security procedures

Objectives

Protecting intelligence information is your priority. When you were granted your security clearance, you were entrusted with safekeeping our country's biggest secrets. As we move through this session, we will explore SCI and the key security methods.

Objectives

- Define SCI, how it is collected, and why it needs to be protected
- Discriminate between clearances and access approvals
- Identify and describe the different security methods
 - Goal and purpose
 - Your personal responsibilities
- Describe the relationship between the characteristics of those who have committed espionage and personnel reporting requirements
- Identify how OPSEC supports you in the execution of your security responsibilities
- Identify the key governing documents that define security procedures

(Image Alt: Four images representing each of the key security disciplines.)

Slide 36

Classification Levels

The DNI is responsible for protecting classified NSI and intelligence sources and methods from unauthorized disclosures. The classification level for NSI 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 NSI, for which only a classification level applies (no additional control markings are necessary), is referred to as "collateral" information.

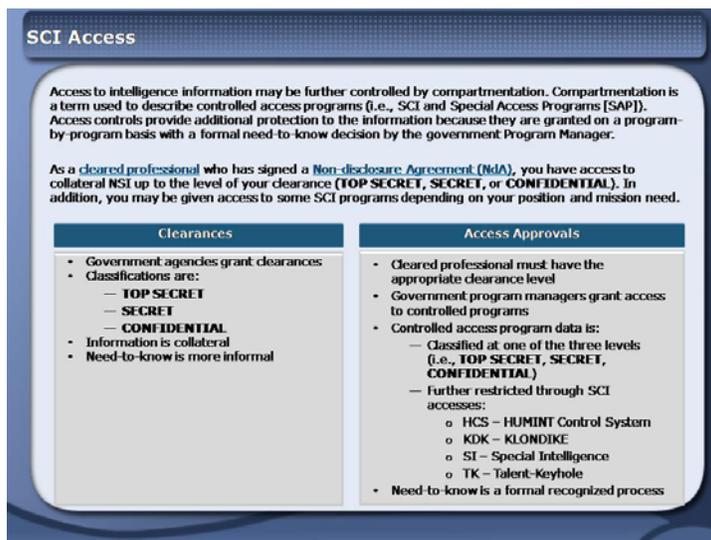
| Classification | Level of Damage |
|-------------------------|----------------------------|
| TOP SECRET (TS) | Exceptionally grave damage |
| SECRET (S) | Serious damage |
| CONFIDENTIAL (C) | Damage |

Classification Levels

The DNI is responsible for protecting classified NSI and intelligence sources and methods from unauthorized disclosures. The classification level for NSI 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 NSI, 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 |

Slide 37



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"> • Government agencies grant them • Classifications are: <ul style="list-style-type: none"> ○ TOP SECRET ○ SECRET ○ CONFIDENTIAL • Information is collateral • Need-to-know is more informal | <ul style="list-style-type: none"> • Cleared professional must have the appropriate clearance level • Government program managers grant access to controlled programs • Controlled access program data is: <ul style="list-style-type: none"> ○ Classified at one of the three levels (i.e., TOP SECRET, SECRET, CONFIDENTIAL) ○ Further restricted |

| | |
|--|--|
| | <p>through SCI accesses:</p> <ul style="list-style-type: none"> ▪ HCS – HUMINT Control System ▪ KDK – KLONDIKE ▪ SI – Special Intelligence ▪ TK – Talent-Keyhole <ul style="list-style-type: none"> • Need-to-know is a formal recognized process |
|--|--|

Pop Up: Cleared Professional

A cleared professional, as defined in *EO 13526*, is an authorized holder of classified NSI. 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.

Pop Up: Non-disclosure Agreement (NdA)

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 NSI
- 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

Slide 38

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.



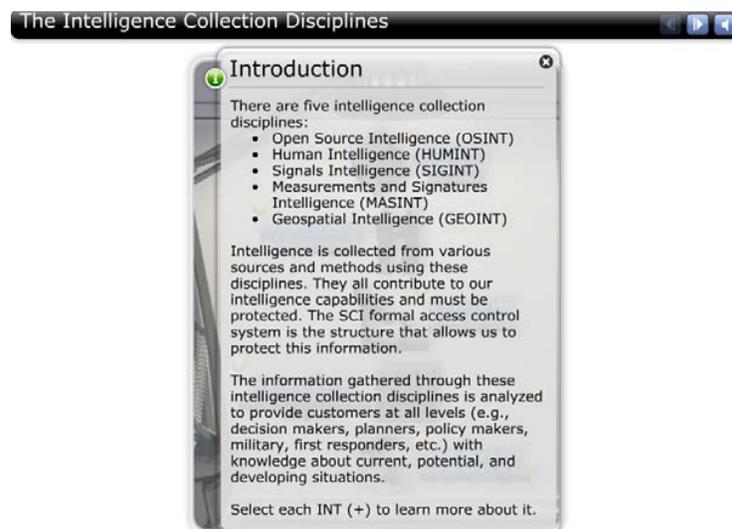
Clearances vs. Accesses

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: Two images. The first showing a woman looking at a hotel map in which the top floors are marked SCI and the remaining floors are marked Collateral. This image represents the floors she goes to with her clearance and access. The second image shows the floors of the hotel labeled (from the bottom up) Confidential, Secret, Top Secret, and SCI. The SCI floors are labeled with SCI compartment on it. There is also a hand with a badge in front of the image. The badge represents the persons' clearances and accesses.)

Slide 39



The Intelligence Collection Disciplines

Introduction

There are five primary intelligence collection disciplines:

- Open Source Intelligence (OSINT)
- Human Intelligence (HUMINT)
- Signals Intelligence (SIGINT)
- Measurement & 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.

OSINT

Open Source Intelligence 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 is intelligence gathering by means of human contact. HUMINT can be overtly or covertly collected.

The NCS of the CIA is responsible for foreign HUMINT operations.

SIGINT

Signals Intelligence 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 & Signature Intelligence 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 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.

Slide 40**Adversary Targets**

Image Alt: Interaction of three concentric circles.

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.](#)

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 include 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:

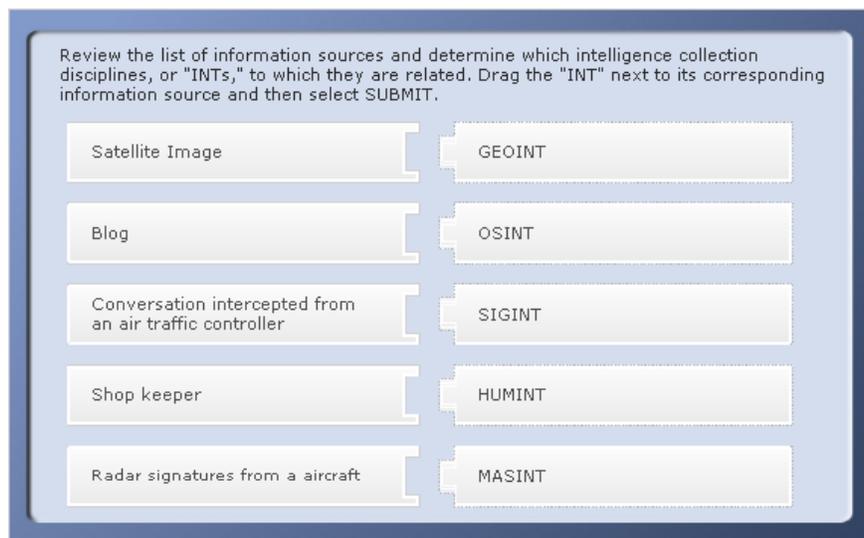
- Our critical infrastructure
- Our critical infrastructure vulnerabilities
- The impact to our society, our government, and the public's confidence in the government, if our critical infrastructure is compromised

Nuclear Capabilities

Nuclear Capabilities include information about:

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

Page 41



Intelligence Collection Disciplines

- 1. Review the list of information sources and determine which intelligence collection disciplines, or "INTs," to which they are related.**

Drag the "INT" next to its corresponding information source and then select SUBMIT.

| Correct | Choice |
|---|--------|
| Satellite Image | GEOINT |
| Blog | OSINT |
| Conversation intercepted from an air traffic controller | SIGINT |
| Shop keeper | HUMINT |
| Radar signatures from a aircraft | MASINT |

Feedback when correct:

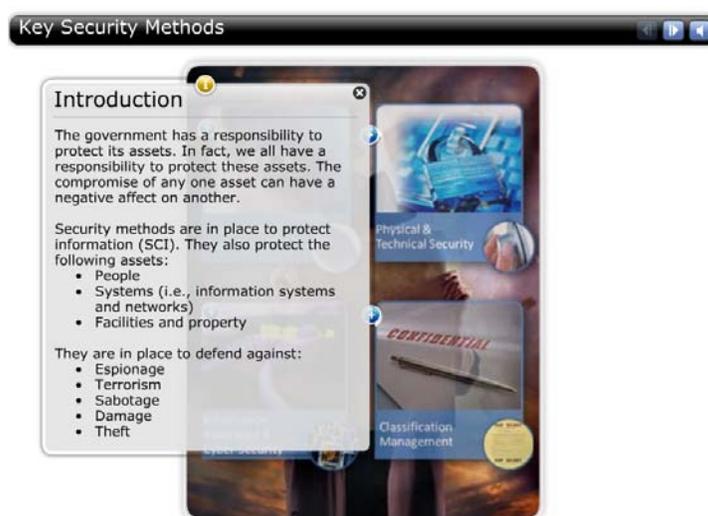
That's right! You selected the correct answers.

- A satellite image is an example of GEOINT
- A blog is an example of OSINT
- A conversation intercepted from an air traffic control tower is an example of SIGINT
- A shop keeper is an example of HUMINT
- Radar signatures from a specific type of aircraft is an example of MASINT

Feedback when incorrect:

You did not select the correct answers.

- A satellite image is an example of GEOINT
- A blog is an example of OSINT
- A conversation intercepted from an air traffic control tower is an example of SIGINT
- A shop keeper is an example of HUMINT
- Radar signatures from a specific type of aircraft is an example of MASINT

Slide 42**Key Security Methods**

(Interaction Alt: Roll over image depicting the four key security methods: Personnel Security, Physical and Technical Security, Information Assurance and Cyber Security, and Classification Management.)

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

Personnel Security (PERSEC)

Personnel Security 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)

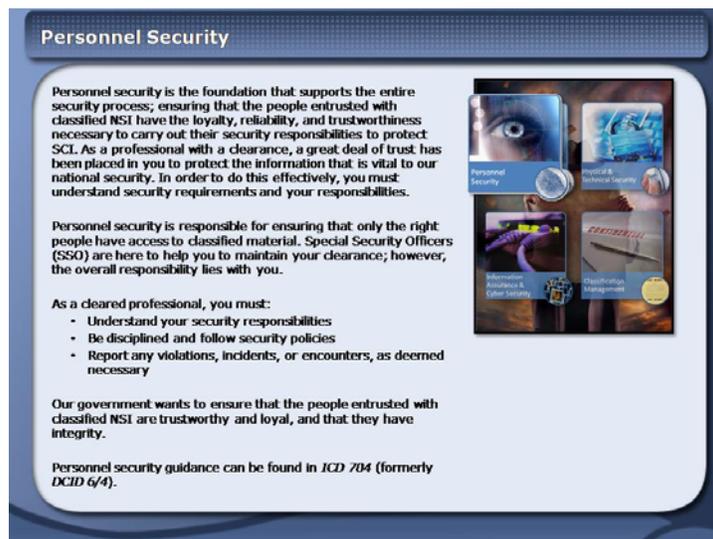
Classification Management

Classification management is the security method that provides the IC procedures for protecting NSI 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, Classified National Security Information; Final Rule

Slide 43



Personnel Security

Personnel security is the foundation that supports the entire security process; ensuring that the people entrusted with classified NSI have the loyalty, reliability, and trustworthiness necessary to carry out their security responsibilities to protect SCI. As a professional with a clearance, a great deal of trust has been placed in you to protect the information that is vital to our national security. In order to do this effectively, you must understand security requirements and your responsibilities.

Personnel security is responsible for ensuring that only the right people have access to classified material. Special Security Officers (SSO) are here to help you to maintain your clearance; however, the overall responsibility lies with you.

As a cleared professional, you must:

- Understand your security responsibilities
- Be disciplined and follow security policies
- Report any violations, incidents, or encounters, as deemed necessary

Our government wants to ensure that the people entrusted with classified NSI are trustworthy and loyal, and that they have integrity.

Personnel security guidance can be found in ICD 704 (formerly DCID 6/4).



Personnel Security

Personnel security is the foundation that supports the entire security process; ensuring that the people entrusted with classified NSI have the loyalty, reliability, and trustworthiness necessary to carry out their security

responsibilities to protect SCI. As a professional with a clearance, a great deal of trust has been placed in you to protect the information that is vital to our national security. In order to do this effectively, you must understand security requirements and your responsibilities.

Personnel security is responsible for ensuring that only the right people have access to classified material. Special Security Officers (SSO) are here to help you to maintain your clearance; however, the overall responsibility lies with you.

As a cleared professional, you must:

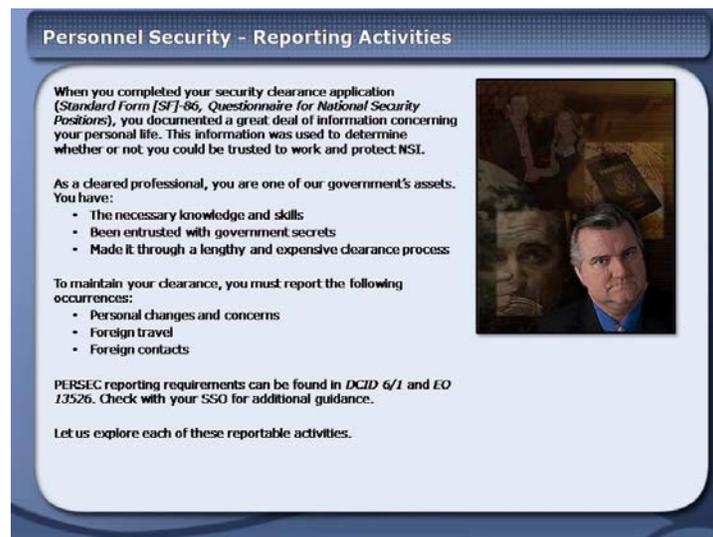
- Understand your security responsibilities
- Be disciplined and follow security policies
- Report any violations, incidents, or encounters, as deemed necessary

Our government wants to ensure that the people entrusted with classified NSI are trustworthy and loyal and that they have integrity.

Personnel security guidance can be found in *ICD 704* (formerly *DCID 6/4*).

(Image Alt: Four images representing each of the key security disciplines. Personnel Security is highlighted.)

Slide 44



Personnel Security - Reporting Activities

When you completed your security clearance application (*Standard Form [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 NSI.

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.

Personnel Security - Reporting Activities

When you completed your security clearance application (*Standard Form [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 NSI.

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:

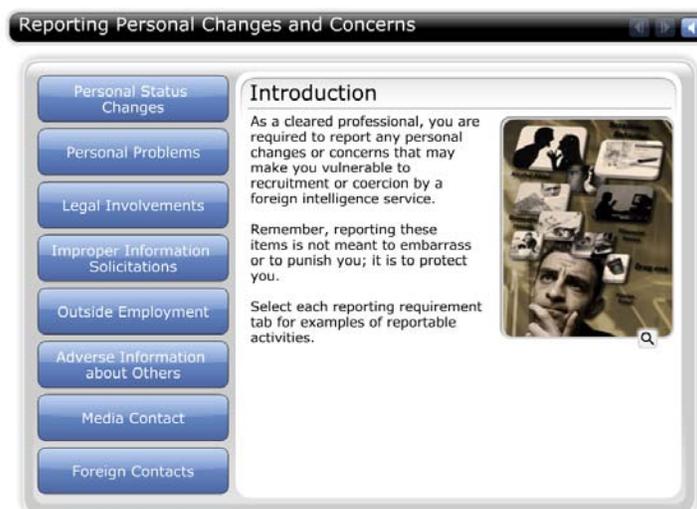
- Personal changes and concerns
- Foreign travel
- Foreign contacts

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 Pat with a variety of reportable activities. These include: foreign travel, interactions with non-US persons, and alcohol abuse.)

Slide 45



Reporting Personal Changes and Concerns

(Interaction Alt: Rollover interaction of changes and concerns with a collage of reportable activities. These include: suspicious behavior, alcohol abuse, domestic issues, financial issues, drug use, and foreign travel.)

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.](#)

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) (such as an arrest for Driving Under the Influence [DUI] of drugs)
- Abuse or misuse of alcohol (such as an arrest for 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.

(Interaction Alt: Collage of reportable activities. These include: suspicious behavior, alcohol abuse, domestic issues, financial issues, drug use, and foreign travel.)

Slide 46

Personnel Security – 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 |

When in doubt, consult with your SSO.

Personnel Security – 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.

Did you know that going to an embassy qualifies as foreign travel?

Slide 47

Personnel Security – 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 |

When in doubt, consult with your SSO.

Personnel Security – Reporting Foreign Contacts

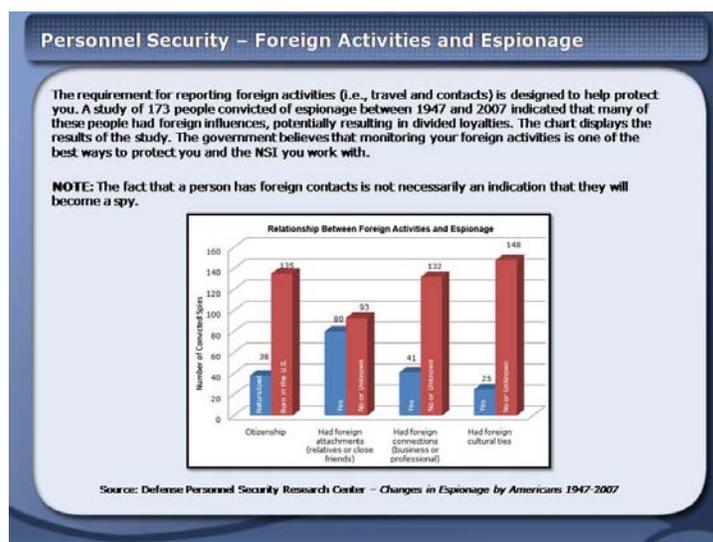
It is not uncommon to come into contact with non-U.S. persons on a daily basis (e.g., professor, doctor, hairdresser, housekeeper, or colleague). The following information specifies when it is necessary to report a foreign contact.

| 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 |

| | | |
|--|--|--|
| | <p>interactions with individuals at a conference</p> <ul style="list-style-type: none"> • Social interactions at a party or gathering | |
|--|--|--|

When in doubt, consult with your SSO.

Slide 48



Personnel Security – 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 NSI you work with.

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

Chart: Relationship Between Foreign Activities and Espionage

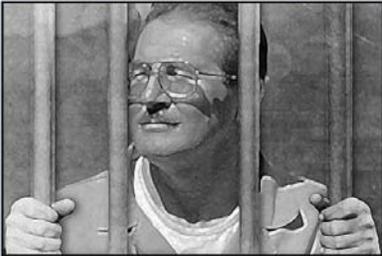
Source: Defense Personnel Security Research Center – *Changes in Espionage by Americans 1947-2007*

(Image Alt: Bar graph that looks some of the characteristics of the 173 people who have been convicted of espionage.)

Slide 49

Espionage in the U.S.

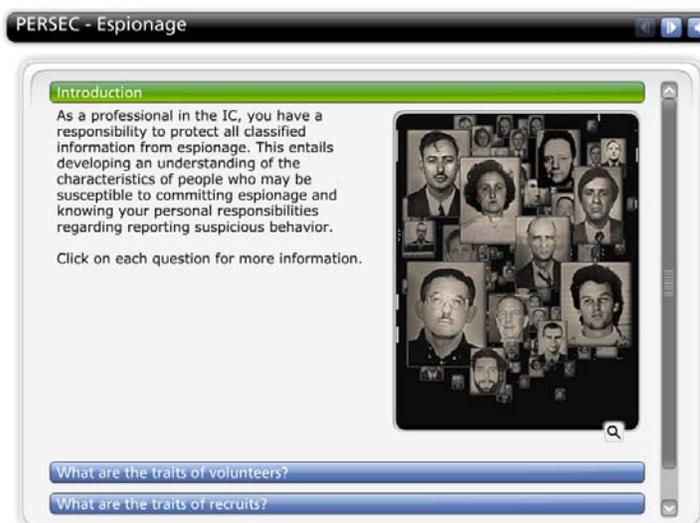
Espionage can be defined as stealing information that governments or organizations are trying to protect. One spy can cause significant damage to intelligence collection by divulging information about our intelligence sources and methods. For example, while Aldrich Ames worked for the CIA, he spied for 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 convicted spy, looking out from behind vertical metal bars. He is wearing glasses and a light-colored shirt.**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 convicted of espionage.)

Slide 50



PERSEC – Espionage

(Interaction Alt: Series of questions. On the main screen, there is a collage of people who have committed 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.](#)

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

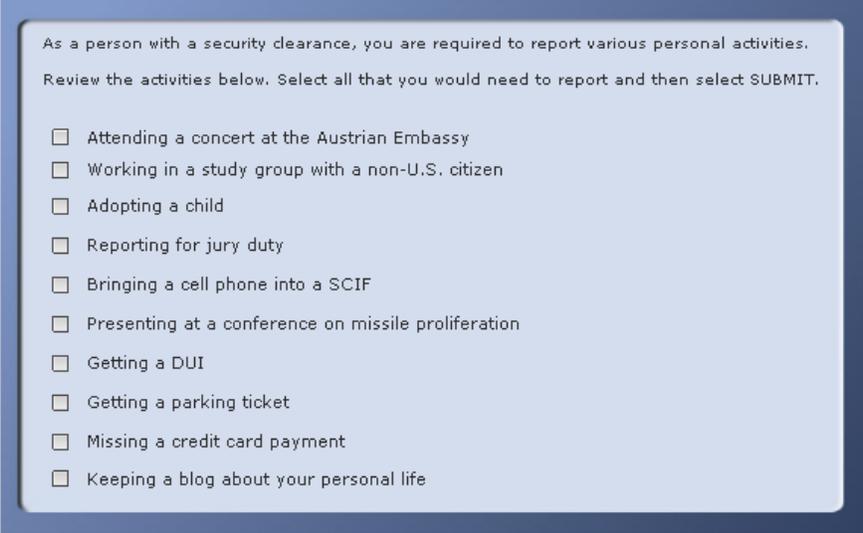
- Are uncomfortable with sexual identity
- Professional Relationships
 - Are not good team players
 - Are good individual contributors
 - Have a hard time getting along with coworkers
- Personal Relationships
 - Have unstable (or no) relationships
 - Do not seek close personal relationships
 - Never 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 SSO and/or manager

Slide 51



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.

- 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

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.](#)

| 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.

Slide 52

Physical and Technical Security

Physical and technical security methods are those that are the most visible – security measures such as formal access controls, locks, Sensitive Compartmented Information Facilities (SCIF), alarms, etc.

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 NSI through communication technologies
- Prevent the compromise of classified NSI 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*.

Physical and Technical Security

Physical and technical security methods are those that are the most visible – security measures such as formal access controls, locks, Sensitive Compartmented Information Facilities (SCIF), alarms, etc.

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

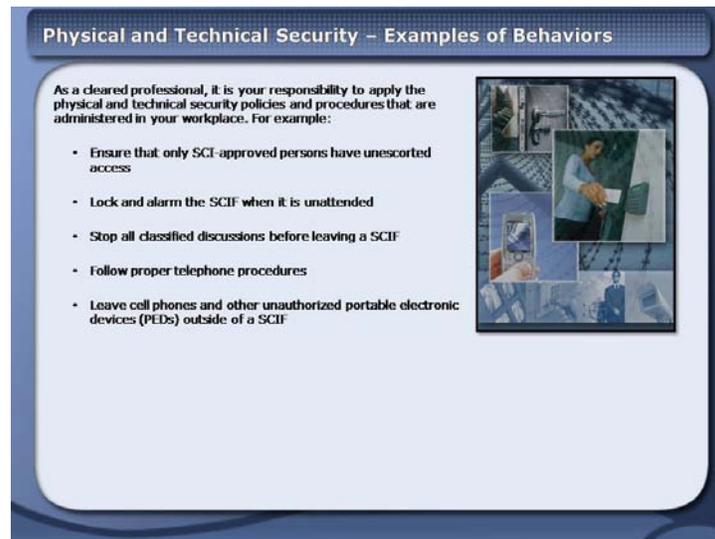
- Protect personnel
- Prevent unauthorized access to facilities, equipment, materials, and documents
- Prevent the compromise of classified NSI through communication technologies
- Prevent the compromise of classified NSI through compromising emanations using TEMPEST, TSCM, and telecommunications security
- 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: Four images representing each of the key security disciplines. Physical Security is highlighted.)

Slide 53



Physical and Technical Security – Examples of Behaviors

As a cleared professional, it is your responsibility to apply the physical and technical security policies and procedures that are administered in your workplace. For example:

- Ensure that only SCI-approved persons have unescorted access
- Lock and alarm the SCIF when it is unattended
- Stop all classified discussions before leaving a SCIF
- Follow proper telephone procedures
- Leave cell phones and other unauthorized portable electronic devices (PEDs) outside of a SCIF

(Image Alt: Collage containing images of physical security measures. These include locks, access controls, identification cards, security guards, barbed wire, not bringing in cell phones, etc.)

Slide 54

Physical and Technical Security – 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's silhouette as they enter a room through a doorway. The room is dimly lit, with several circular lights on the ceiling. The person is walking away from the camera into the room.**Physical and Technical Security – 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.

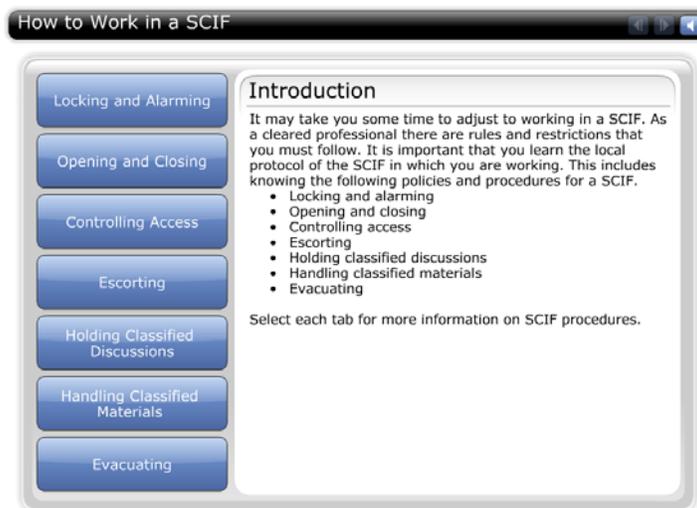
An unattended SCIF is always locked and alarmed. Some are guarded and staffed around the clock and do not close.

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 man walking into a high security room (SCIF).)

Slide 55



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 for that SCIF (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

Slide 56

Physical and Technical Security - 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 essential to ensuring 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.



The diagram is a pyramid divided into four segments. The top segment is green and labeled 'PEDs'. The middle section is divided into two blue segments: 'Non-Secure Telephones' on the left and 'Secure Telephones' on the right. The bottom segment is red and labeled 'Secure Telephone Systems'.

Personal Responsibilities

(Interaction Alt: Pyramid roll over with three layers and four segments)

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.

PEDs

Portable Electronic Devices 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

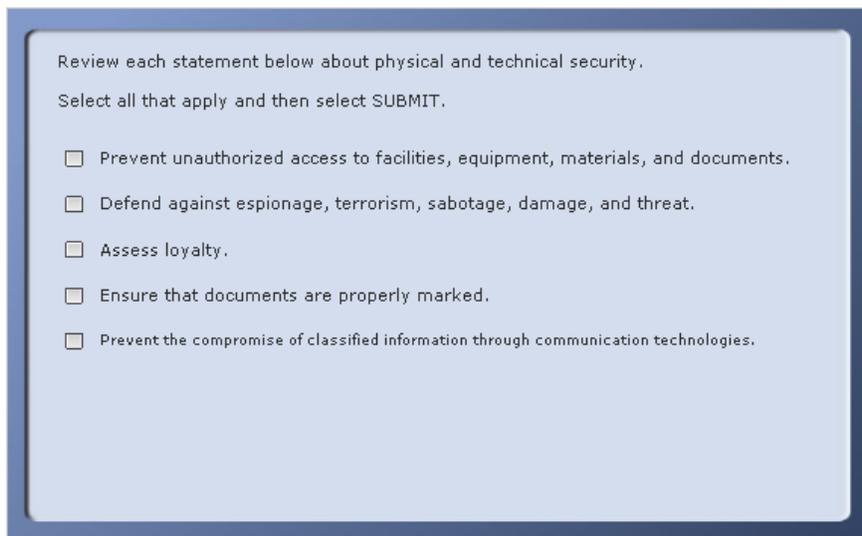
Secure telephones have been certified to handle classified conversations. Secure Telephone Equipment (STE) is any instrument that has been certified to handle classified information. The encryption takes place at the instrument and requires certain actions by the user for the phone to be in secure mode.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

- Use the appropriate keying device and/or press the secure button to ensure that your conversation is encrypted
- Check the Light Emitting Diode (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.

Slide 57



Knowledge Check - Physical and Technical Security

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

Select all that apply and then select SUBMIT.

| 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.

Slide 58

Information Assurance and Cyber Security

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

Information Assurance and Cyber Security

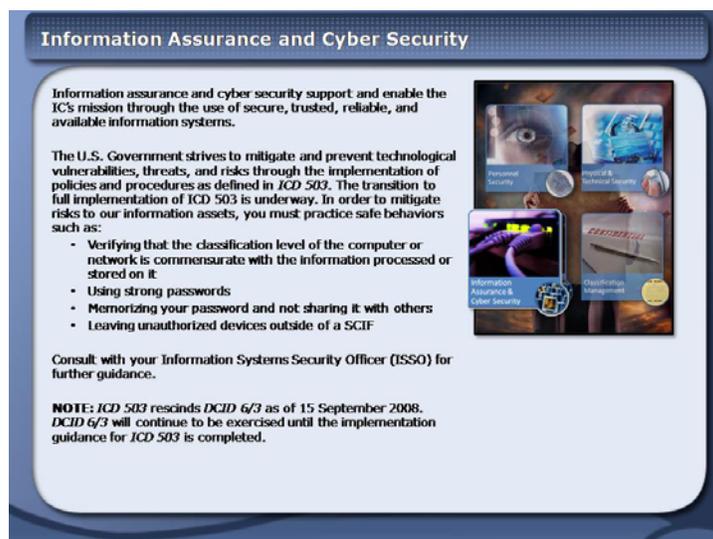
Information assurance and cyber security have become increasingly important as more work is carried out in the digital and cyber arenas. Because cyber and digital threats are always changing, security policies and procedures can only do so much to protect against them. As a user of government systems 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

(Image Alt: Four images representing each of the key security disciplines. The image of Information Assurance and Cyber Security is highlighted.)

Slide 59



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*. The transition to full implementation of *ICD 503* is underway. 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.

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*. The transition to full implementation of *ICD 503* is underway. In order to mitigate risks to our information assets, you must practice safe behaviors such as:

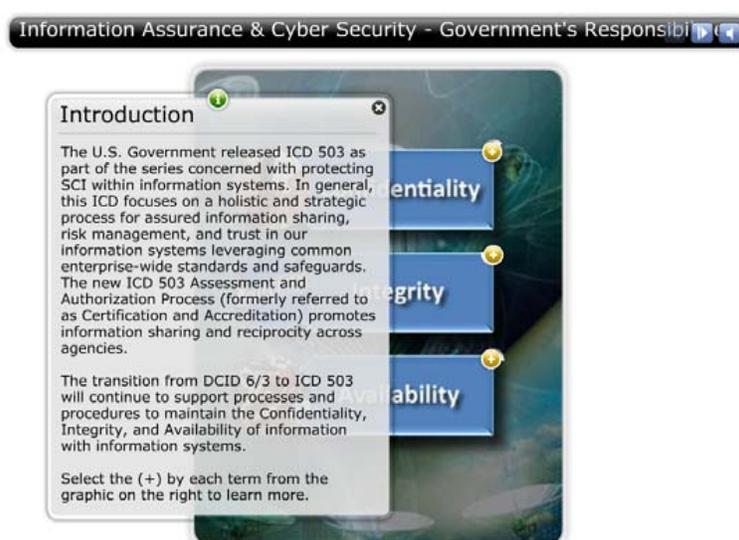
- Verifying that the classification level of the computer or network is commensurate with the information processed or stored on it
- Using strong passwords
- Memorizing your password and not sharing it with others
- Leaving unauthorized devices outside of a SCIF

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: Four images representing each of the key security disciplines. The image of Information Assurance and Cyber Security is highlighted.)

Slide 60



Government's Responsibilities

(Interaction Alt: Roll over interaction segmented to show confidentiality, integrity, and availability)

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.

Confidentiality

(Image Alt: person whispering in someone else's ear)

The assurance that information is not accessible to:

- Unauthorized individuals
- Processes
- Devices

Integrity

(Image Alt: Street sign with Integrity written on it.)

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

Availability

(Image Alt: Hand picking an apple.)

The assurance that information is available and accessible when needed.

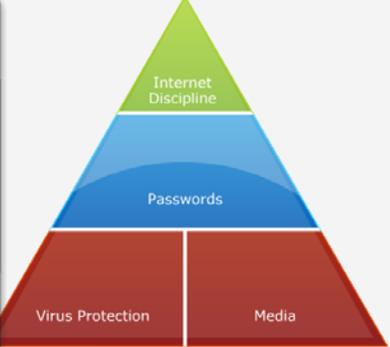
Slide 61

Information Assurance & Cyber Security - Personal Responsibilities

Introduction

The 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. 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:

- On classified and unclassified networks
- On computers, smart phones, cell phones, PDAs,



Personal Responsibilities

(Interaction Alt: pyramid segmented into six segments.)

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.](#)

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

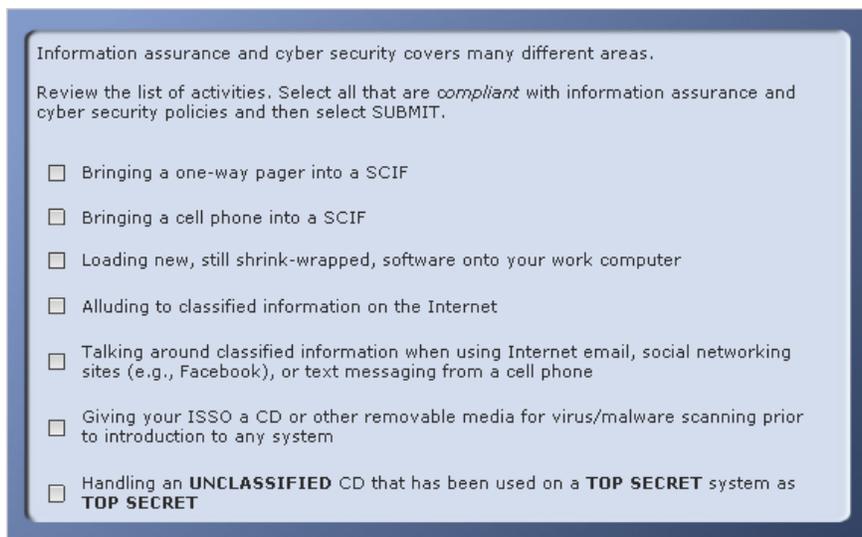
Media

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 controlled at the highest level. For example, if you put an unclassified CD into a **TOP SECRET** computer, the CD becomes controlled at the **TOP SECRET** level even though no content on it has changed.

Slide 62



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.](#)

| 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.

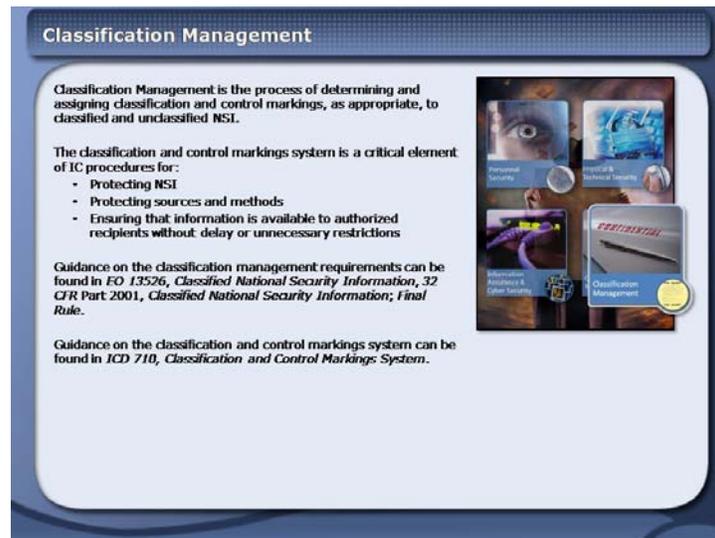
The following activities are compliant with information assurance and cyber security policies.

- 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.

Slide 63

Classification Management

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

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

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

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*.

The graphic on the right shows four overlapping images representing key security disciplines: 'Personal Security' (eye), 'ICD 710' (document), 'Information Assurance & Cyber Security' (circuit board), and 'Classification Management' (document with 'ESSENTIAL' stamp).

Classification Management

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

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

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

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*.

(Image Alt: Four images representing each of the key security disciplines. Classification Management is highlighted.)

Slide 64

Purpose of Classification Management

The classification and control markings system provides a uniform system for classifying, safeguarding, and declassifying NSI.

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 NSI. Proper application of markings supports effective protection and safeguarding, and expedites information sharing across agencies.

**Purpose of Classification Management**

The classification and control markings system provides a uniform system for classifying, safeguarding, and declassifying NSI.

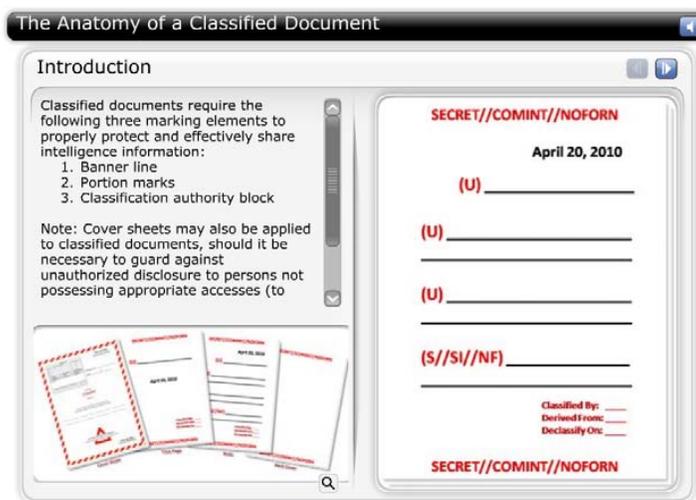
The classification and control markings system communicates one or more of the following:

- 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 NSI. Proper application of markings supports effective protection and safeguarding, and expedites information sharing across agencies.

(Image Alt: Collage of mock-up of classified documents that are marked with the appropriate classification, portions marks, marked with the word confidential and floppy disk.)

Slide 65



The Anatomy of a Classified Document

(Interaction Alt: Mock-up of a classified document that is marked with the appropriate classification and portion marks.)

Introduction

(Image Alt: Different components that may go into a classified document: Cover sheet, top page, page, and back cover.)

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.

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 Communications Intelligence (**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.

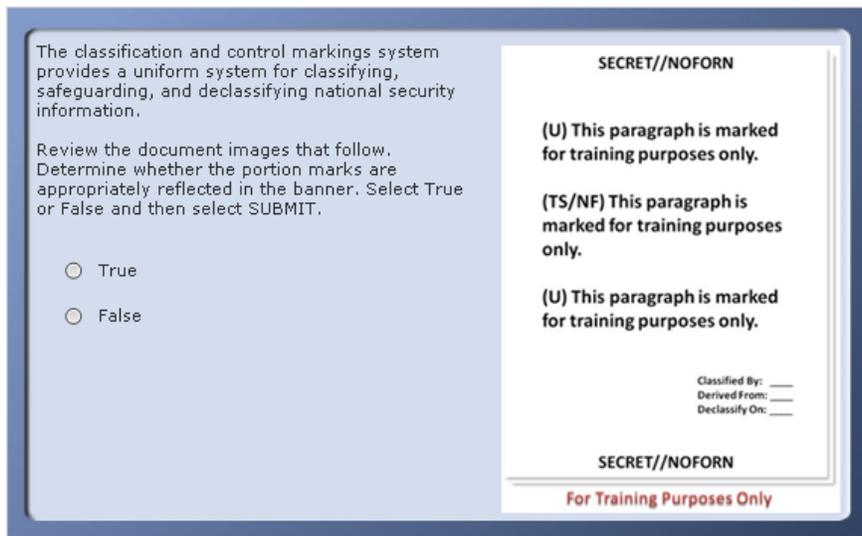
There are two forms of authority blocks:

- Original Classification Authority (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)

Slide 66



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.](#)

| 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.

| 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.

| 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**.

| 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*.

Slide 67

OPSEC and the Key Security Methods

OPSEC is the process of identifying unclassified activities and information and evaluating the potential those might have in revealing classified NSI. 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.ioss.gov) from the Course Resources.



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

OPSEC and the Key Security Methods

OPSEC is the process of identifying unclassified activities and information and evaluating the potential those might have in revealing classified NSI. 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.ioss.gov) from the Course Resources.

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

(Image Alt: Man walking down a busy street with his badge around his neck. He is carrying classified materials in a lock bag. There is someone watching.)

Slide 68

Additional Responsibilities

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.

A portrait of a man with grey hair, wearing a dark suit, a blue shirt, and a patterned tie. He is smiling slightly and looking towards the camera. The background is a blurred office setting.**Additional Responsibilities**

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.

(Image Alt: Pat standing in his office.)

Slide 69

Additional Responsibilities – Unauthorized Disclosures

You are responsible for protecting classified information from unauthorized disclosures. An unauthorized disclosure is a communication or physical transfer of NSI, 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.

**Additional Responsibilities – Unauthorized Disclosures**

You are responsible for protecting classified information from unauthorized disclosures. An unauthorized disclosure is a communication or physical transfer of NSI, 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: Man passing a folder containing classified information to a woman on a park bench.)

Slide 70

Additional Responsibilities – Reporting Unauthorized Disclosures

If you become aware of, or suspect, an unauthorized disclosure of classified NSI, 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."

Reporting Unauthorized Disclosures

If you become aware of, or suspect, an unauthorized disclosure, security violation, or compromise of NSI, 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)

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

**Additional Responsibilities – Reporting Unauthorized Disclosures**

If you become aware of, or suspect, an unauthorized disclosure of classified NSI, 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."

Reporting Unauthorized Disclosures

If you become aware of, or suspect, an unauthorized disclosure, security violation or compromise of NSI, 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)

Remember

Do not discuss this with anyone but your immediately supervisor or SSO.

(Image Alt: Pat looking stern.)

Slide 71

Additional Responsibilities – 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.



NOTE: 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.

Additional Responsibilities – 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:

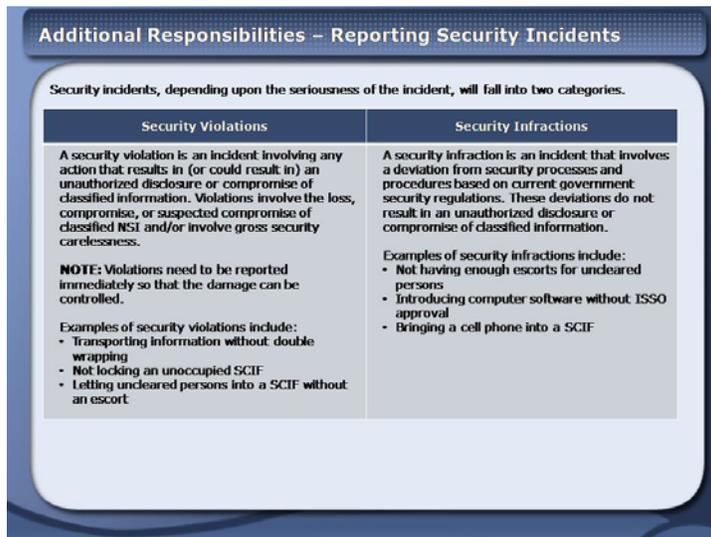
- Speeches, articles, white papers, advertisements, etc.
- Web pages, web sites, blogs, chat rooms, video teleconferences, etc.

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

NOTE: 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: Pre-publication review meeting. Two members are holding up cards casting their opposing votes on whether or not to allow a document for publication.)

Slide 72



Additional Responsibilities – Reporting Security Incidents

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

| Security Violations | Security Infractions |
|--|---|
| <p>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 NSI and/or involve gross security carelessness.</p> <p>NOTE: Violations need to be reported immediately so that the damage can be controlled.</p> <p>Examples of security violations include:</p> <ul style="list-style-type: none"> • Transporting information without double wrapping • Not locking an unoccupied SCIF • Letting uncleared persons into a SCIF without an escort | <p>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.</p> <p>Examples of security infractions include:</p> <ul style="list-style-type: none"> • Not having enough escorts for uncleared persons • Introducing computer software without ISSO approval • Bringing a cell phone into a SCIF |

Slide 73

Additional Responsibilities – Reporting Security Incidents (cont.)

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.

Administrative and Criminal Sanctions

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

Additional Responsibilities – Reporting Security Incidents (cont.)

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.

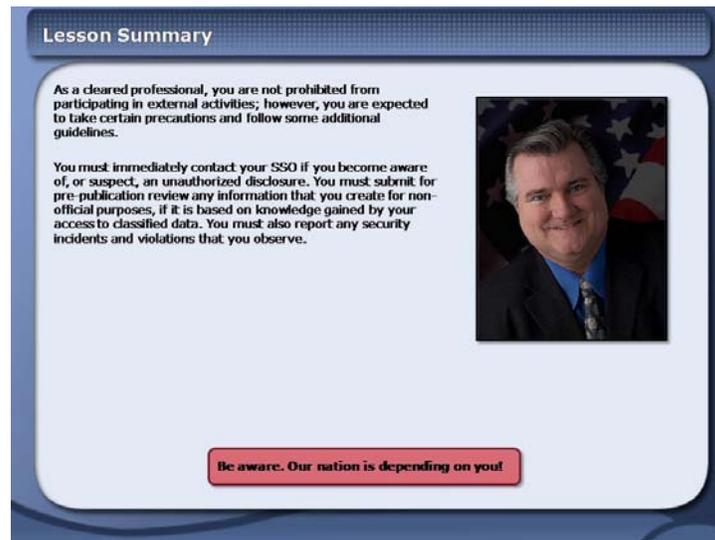
Pop Up Suspicious co-Worker Activities

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

Slide 74



Lesson 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.

Be aware. Our nation is depending on you!

The slide features a blue header with the title 'Lesson Summary'. The main content area is white with a blue border. On the right side, there is a portrait of a man in a suit and tie, standing in front of an American flag. At the bottom, there is a red button with white text that reads 'Be aware. Our nation is depending on you!'.

Lesson 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.

Be aware. Our nation is depending on you!

(Image Alt: Pat standing in front of an American flag.)

Slide 75**Lesson 2: Scenario**

(Approximately 20 Minutes)

(Alt Image: Title Slide with ODNI seal.)

Slide 76A blue-themed slide titled "Lesson Introduction" in a white box at the top. The main content area is white with blue text. On the right side, there is a graphic of a blue circular "Inbox" icon with the text "Inbox 1" and "Started" on it. Below the icon, the text "You've got mail." is displayed. The slide contains several paragraphs of instructional text.

Lesson Introduction

Now that you have reviewed the security polices, it is time to apply them to your job by completing the following scenario. Scenarios provide realistic situations in which you can practice and apply what you have learned.

Put yourself in the following fictitious scenario where you are asked to plan a special symposium for attendees from across the IC.

You are playing the role of an Event Planner, who needs to coordinate a classified symposium. You need to work with your SSO and stakeholders to organize the symposium and collect requirements for the logistics of the classified event. Throughout this scenario, and with the guidance and help from your scenario SSO, you will apply the security skills that you learned in Lesson 1, to the planning of the symposium.

Click on the Inbox graphic to open the email.

Inbox 1
Started

You've got mail.

Lesson Introduction

Now that you have reviewed the security polices, it is time to apply them to your job by completing the following scenario. Scenarios provide realistic situations in which you can practice and apply what you have learned.

Put yourself in the following fictitious scenario where you are asked to plan a special symposium for attendees from across the IC.

You are playing the role of an Event Planner who needs to coordinate a classified symposium. You need to work with your SSO and stakeholders to organize the symposium and collect requirements for the logistics of the classified event. Throughout this scenario, and with the guidance and help from your scenario SSO, you will apply the security skills that you learned in Lesson 1 to the planning of the symposium.

[Click on the Inbox graphic to open the email.](#)

(Alt Image: e-mail inbox)

Pop Up: Inbox Graphic

To: Sent: March 14
From: Susan
Subject: New Task – Symposium

Good morning!

I was just meeting with Casey, my counterpart at the DHS. We were discussing the attempted terrorist attack on December 25, 2009. She told me about a paper that Ray, one of her colleagues, had written discussing the use of facial recognition software at airport security checkpoints. We would like Ray to present his classified paper at a special symposium to be held in our SCIF Conference Center this June. I would like you to set up the event, arrange for the logistics, and coordinate with security to ensure the success of the event.

Do you have time to meet tomorrow and go over the requirements?

Susan
Chief, Terrorism Unit

Slide 77

Project Notification – Meeting with Susan

You go to meet with Susan, your manager, to flesh out the requirements and to obtain her input.

On December 25, 2009, a Nigerian citizen boarded a U.S. plane from Amsterdam bound for Detroit, Michigan. This was no ordinary traveler; the individual was a terrorist with an explosive device contained in his underwear. He passed through the security screening without causing alarm. Luckily, his effort was unsuccessful. The device failed to ignite properly and other brave passengers thwarted his attack.

Since the incident, there has been a lot of discussion about using whole-body scanners as a replacement for the traditional metal detectors. However, these scanners are expensive and controversial. The U.S. Federal Government is looking for viable, alternative solutions. Ray has written a classified white paper (TS//HCS/SI/TK//NOFORN) proposing a solution.

A small portrait photograph of a woman with dark hair, wearing a dark blazer, smiling slightly. She is identified as Susan in the alt text.**Project Notification – Meeting with Susan**

You go to meet with Susan, your manager, to flesh out the requirements and to obtain her input.

On December 25, 2009, a Nigerian citizen boarded a U.S. plane from Amsterdam bound for Detroit, Michigan. This was no ordinary traveler; the individual was a terrorist with an explosive device contained in his underwear. He passed through the security screening without causing alarm. Luckily, his effort was unsuccessful. The device failed to ignite properly and other brave passengers thwarted his attack.

Since the incident, there has been a lot of discussion about using whole-body scanners as a replacement for the traditional metal detectors. However, these scanners are expensive and controversial. The U.S. Federal Government is looking for viable, alternative solutions. Ray has written a classified white paper (TS//HCS/SI/TK//NOFORN) proposing a solution.

(Alt Image: Susan)

Slide 78

Project Notification – Meeting with Susan (continued)



I need to you coordinate the preparation of a special symposium, sponsored by DHS, on improving the security of our borders. It will be held in June at our SCIF Conference Center. Ray, a DHS employee, will be presenting his classified white paper (TS//HCS//SI//TK//NOFORN) discussing the use of facial recognition software to identify known terrorist suspects. He will present the approach that is described in his classified paper at the symposium.

The symposium will be held at the TS//SI//TK level; note that this is different than the classification and compartmentation of the white paper. However, we want all the attendees to be able to listen to Ray's presentation and discuss the feasibility and implementation of his ideas. You need to make the event as seamless as possible for all involved.

To sum up, I am tasking you with the overall coordination and logistics for the TS//SI//TK symposium.

Project Notification – Meeting with Susan (continued)

I need to you coordinate the preparation of a special symposium, sponsored by DHS, on improving the security of our borders. It will be held in June at our SCIF Conference Center. Ray, a DHS employee, will be presenting his classified white paper (TS//HCS//SI//TK//NOFORN) discussing the use of facial recognition software to identify known terrorist suspects. He will present the approach that is described in his classified paper at the symposium.

The symposium will be held at the TS//SI//TK level; note that this is different than the classification and compartmentation of the white paper. However, we want all the attendees to be able to listen to Ray's presentation and discuss the feasibility and implementation of his ideas. You need to make the event as seamless as possible for all involved.

To sum up, I am tasking you with the overall coordination and logistics for the TS//SI//TK symposium.

(Alt Image: Susan)

Slide 79

Event Planning Activities

After your meeting with Susan, you identify the key activities that you need to conduct prior to the event.



The image shows a bulletin board with three yellow sticky notes pinned to it. The first note says '1. DEFINE AND ESTABLISH REQUIREMENTS', the second says '2. FINALIZE LOGISTICS', and the third says '3. CREATE PRE-SYMPOSIUM PACKAGE'. There is also a small photograph of a landscape on the board.

Event Planning Activities

After your meeting with Susan, you identify the key activities that you need to conduct prior to the event.

(Alt Image: Bulletin board with three sticky notes on it describing the tasks to be done: 1. Define and Establish Requirements, 2. Finalize Logistics, and 3. Create Pre-Symposium Packet.)

Slide 80

Define and Establish Requirements

To properly define and establish the requirements for the event, you decide to talk with all of the stakeholders involved. You need to:

- Meet with Casey, symposium host
- Meet with Pat, SSO
- Meet with Ray, author and presenter



The image shows a bulletin board with three yellow sticky notes pinned to it. The first note says '1. DEFINE AND ESTABLISH REQUIREMENTS', the second says '2. FINALIZE LOGISTICS', and the third says '3. CREATE PRE-SYMPOSIUM PACKAGE'. There is also a small photograph of a landscape on the board.

Define and Establish Requirements

To properly define and establish the requirements for the event. You decide to talk with all of the stakeholders involved. You need to:

- Meet with Casey, symposium host
- Meet with Pat, SSO
- Meet with Ray, author and presenter

(Alt Image: Bulletin board with only one sticky note on it – 1. Define and Establish Requirements.)

Slide 81



Establish Requirements – Meeting with Casey

Casey, the symposium host, meets with you to discuss the symposium requirements.

Hello!
Susan told me that you will be in charge of running the symposium. I am so glad that you are onboard. Susan said that you have a large conference room in your SCIF that will be able to accommodate us. The content of the symposium is not to go above TS//SI//TK, which is the common access level of all the attendees.

I have already identified and invited the 25 attendees that I want to attend the event. They all have 28 June marked on their calendars and have been told that they will need to send their clearances and appropriate accesses, but they are expecting more details to come. I need you to send them a pre-symposium packet providing them with the logistical information and pre-reading materials for the event. I will send you the information in an email.

Please go ahead and contact Ray for additional information.

Please let me know if you need anything else.

Establish Requirements – Meeting with Casey

Casey, the symposium host, meets with you to discuss the symposium requirements.

Hello!

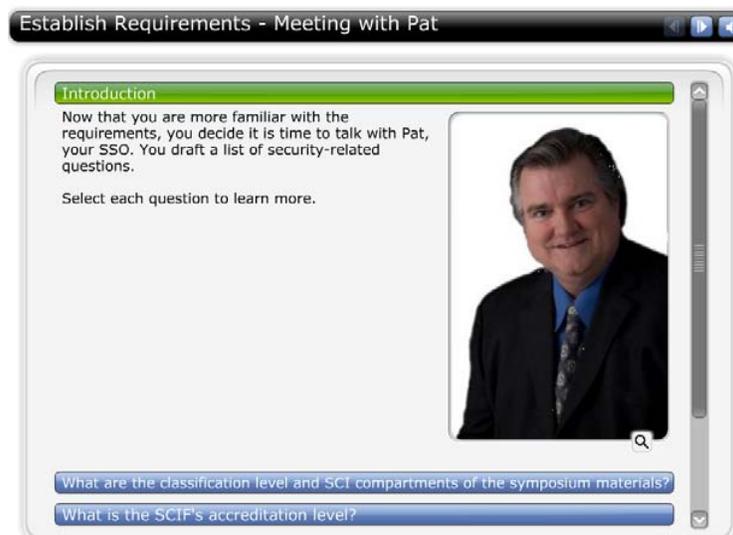
Susan told me that you will be in charge of running the symposium. I am so glad that you are onboard. Susan said that you have a large conference room in your SCIF that will be able to accommodate us. The content of the symposium is not to go above TS//SI//TK, which is the common access level of all the attendees.

I have already identified and invited the 25 attendees that I want to attend the event. They all have 28 June marked on their calendars and have been told that they will need to send their clearances and appropriate accesses, but they are expecting more details to come. I need you to send them a pre-

symposium packet providing them with the logistical information and pre-reading materials for the event. I will send you the information in an email. Please go ahead and contact Ray for additional information. Please let me know if you need anything else.

(Alt Image: Casey)

Slide 82



Establish Requirements - Meeting with Pat

(Alt Interaction: Question interaction. Review each question below)

Introduction

Now that you are more familiar with the requirements, you decide it is time to talk with Pat, your SSO. You draft a list of security-related questions.

[Select each question to learn more.](#)

What are the classification level and SCI compartments of the symposium materials?

Great question, your host and presenter will be able to identify the classification level and SCI compartments of the materials including the presentation and pre-symposium packet. Be sure to inform them of the compartments that the SCIF is accredited to handle.

What is the SCIF's accreditation level?

The SCIF's accreditation level is the classification level and accesses of information that can be processed and stored within the SCIF. The SCIF is

accredited to handle **TOP SECRET** information within HCS, SI, and TK compartments.

Does a pre-publication review of the materials need to take place?

I believe that because the information is being distributed in an official capacity to authorized individuals, a pre-publication review will not be needed. However, this is a question you will need to ask the conference host and presenter.

What clearance level and accesses will the attendees need to attend the symposium?

The attendees will need to have the appropriate accesses and clearances for the materials to which they will be exposed. Since the SCIF is accredited to a TS//HCS//SI//TK level, any attendee not possessing these will need to be escorted within the SCIF Conference Center.

What is the policy for using PEDs and storable media in the Conference Center?

Since the Conference Center is a SCIF, no PEDs are allowed.

What is the process for bringing media into the SCIF and loading it onto a classified system?

The SCIF Conference Center follows the motto "Once in a SCIF, always in a SCIF." Any media that is introduced to the SCIF must be provided to the ISSO. If the classified information is on a CD, the ISSO will virus scan it prior to loading it onto the computer.

However, the easiest thing to do is to have the presenter send the presentation to you using classified e-mail. You can just download it directly to the computer you will be using at the symposium.

Slide 83

Establish Requirements – Meeting with Ray

Ray, the author of the white paper, discusses his paper and requirements with you.

I talked with Casey. I am so glad that you will be helping with the symposium. Let me give you some background information.

I have been working on a white paper that proposes the use of facial recognition software to identify known terrorist suspects. The approach looks at enhancing existing technologies (e.g., cameras, screeners, metal detectors, computers, Internet, etc.) using additional software, connectivity, and trained personnel. This requires improving collaboration and communication between the TSA, DHS Office of Intelligence and Analysis, NCTC, FBI, Department of State, and a few others.

The paper is classified at the TS//HCS//SI//TK//NOFORN level. I have been told that the event cannot include HCS information, so when I create the briefing, I will make sure that HCS is not included. I will go ahead and have the material reviewed so that the information is appropriate for the audience. Before the event, I will send you the presentation over the classified network. Please have it loaded on the appropriate computer for the day of the symposium.

Do you need anything else from me?

**Establish Requirements – Meeting with Ray**

Ray, the author of the white paper, discusses his paper and requirements with you.

I talked with Casey. I am so glad that you will be helping with the symposium. Let me give you some background information.

I have been working on a white paper that proposes the use of facial recognition software to identify known terrorist suspects. The approach looks at enhancing existing technologies (e.g., cameras, screeners, metal detectors, computers, Internet, etc.) using additional software, connectivity, and trained personnel. This requires improving collaboration and communication between the TSA, DHS Office of Intelligence and Analysis, NCTC, FBI, Department of State, and a few others.

The paper is classified at the TS//HCS//SI//TK//NOFORN level. I have been told that the event cannot include HCS information, so when I create the briefing, I will make sure that HCS is not included. I will go ahead and have the material reviewed so that the information is appropriate for the audience. Before the event, I will send you the presentation over the classified network. Please have it loaded on the appropriate computer for the day of the symposium.

Do you need anything else from me?

(Alt Image: Ray)

Slide 84



Summarize Requirements

After your meetings, you create a summary of the requirements and send it in an email to the team.

Click on the Inbox graphic to open the summary email.

(Alt Image: e-mail Inbox)

Pop Up: Inbox Graphic

To: Susan, Casey, Ray, SSO

Sent: March 15

From:

Subject: Facial Recognition Symposium Requirements

Good afternoon!

I just finished meeting with many of you and I wanted to summarize the symposium requirements to ensure that I captured them correctly. Please review and confirm the information below.

Date and Time: June 28; 0800-1200

Location: SCIF Conference Center

Classification: TOP SECRET//SI//TK//NF

Host Agency: DHS

Number of Attendees: 25

Attendees' Clearances: TOP SECRET with various SCI accesses

Attendees' Agencies/Organizations:

- TSA
- DHS, Office of Intelligence and Analysis
- NCTC

- FBI
 - Department of State
-
- Ray's primary responsibilities are to prepare and present the symposium materials. This will include ensuring that the content is at the appropriate security level.
 - Pat's primary responsibilities are to ensure that the security requirements within the SCIF are implemented.
 - My primary responsibilities are to arrange and verify logistics for the symposium.

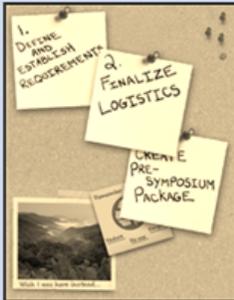
Slide 85

Finalize the Logistics

You have met with the major stakeholders for the event. You understand the requirements for the symposium. Casey has faxed over a list of attendees. You will need to review the list of attendees and determine those needing an escort.

Remember that the SCIF is accredited to the TS//HCS//SI//TK level.

Select NEXT to continue.



Finalize Logistics with SSO

(Alt Image: Bulletin board with only three sticky notes on it – 1. Define and Establish Requirements. 2. Finalize Logistics. 3. Create Pre-Symposium Package.)

(Alt Interaction: Several slide interaction.)

Finalize the Logistics

You have met with the major stakeholders for the event. You understand the requirements for the symposium. Casey has faxed over a list of attendees. You will need to review the list of attendees and determine those needing an escort.

Remember that the SCIF is accredited to the TS//HCS//SI//TK level.

Select **NEXT** to continue.

Review the list of attendees and their clearances and accesses, select those needing an escort, and then select SUBMIT.

| Correct | Choice |
|---------|-----------------------------|
| | Abigail has TS//HCS//SI//TK |
| X | Alexandra has TS//SI//TK |
| | Casey has TS//HCS//SI//TK |
| | Daniel has TS//HCS//SI//TK |
| X | Jean has TS//SI//TK |
| | Sam has TS//HCS//SI//TK |

Feedback when correct:

That's right! You selected the correct responses.

Alexandra and Jean will need an escort within the SCIF. While they have a **TOP SECRET** clearance and SCI accesses, they do not have the HCS access.

Feedback when incorrect:

You did not select the correct response.

Only Alexandra and Jean will need an escort within the SCIF. While they have a **TOP SECRET** clearance and SCI accesses, they do not have the HCS access.

Escorting Tips

Because some of the attendees at the symposium do not have the HCS access to which the SCIF is accredited, they will need to be escorted while inside.

Remember these tips when you escort a person in the SCIF:

- Have an adequate number of escorts
- Keep all attendees needing an escort in your visual control at all times
- Ensure that the escort is as technically competent as those being escorted
- Ensure that Escort Required badges are worn by attendees needing an escort
- Remind all attendees that no HCS information may be presented or discussed

Page 86

Pre-Symposium Packet Requirements

The symposium is just six weeks away. It is time for you to create the pre-symposium packets which will include the following information:

1. Welcome Letter
 - Symposium Information
 - Procedures for passing clearance/accesses
 - Regulations concerning PEDs or storable media
 - Instructions for taking notes and transporting classified information
2. Classified Pre-reading Material

Select NEXT to continue.

The slide features a graphic of a bulletin board with three sticky notes: '1. DEFINE AND ESTABLISH REQUIREMENTS', '2. FINALIZE LOGISTICS', and '3. CREATE PRE-SYMPOSIUM PACKAGE'. There is also a small photo of a landscape on the board.

Create Pre-Symposium Packet

(Alt Image: Bulletin board with only three sticky notes on it – 1. Define and Establish Requirements. 2. Finalize Logistics. 3. Create Pre-Symposium Package.)

(Alt Interaction: Several slide interaction.)

Introduction**Pre-Symposium Packet Requirements**

The symposium is just six weeks away. It is time for you to create the pre-symposium packets which will include the following information:

1. Welcome Letter
 - Symposium Information
 - Procedures for passing clearance/accesses
 - Regulations concerning PEDs or storable media
 - Instructions for taking notes and transporting classified information

2. Classified Pre-reading Material

Select NEXT to continue.

Create the Welcome Letter for the Pre-Symposium Packet

Create a Welcome Letter like the one on the right.

To create the Welcome Letter you will need to:

- Review the sample Welcome Letter
- Review procedures/instructions concerning PEDs and storable media and classified discussions and notes
- Select the most appropriate statement for use in the letter
- Select SUBMIT

Portable Electronic Devices (PEDS) and Storable Media

The Conference Center at which the symposium is being held is a multi-room SCIF, therefore there are restrictions about the use of PEDs (e.g., cell phones, MP3 players, cameras) and portable media (e.g. thumb drives, floppy disks, external hard drives).

Review the statements below, [select the most appropriate one to put in your pre-symposium packet, and then select SUBMIT.](#)

| Correct | Choice | Feedback |
|---------|--|---|
| X | PEDs (e.g., cell phones, MP3 players, cameras) and storable media (e.g. thumb drives, floppy disks, external hard drives) are not permitted in the SCIF Conference Center at all. Please make sure that you leave them in your car. | That's right! You selected the correct response. Since the entire Conference Center is a SCIF, PEDs and storable media are not permitted in a SCIF and must be left outside of the SCIF Conference Center. |
| | PEDs (e.g., cell phones, MP3 players, cameras) and storable media (e.g. thumb drives, floppy disks, external hard drives) are not permitted in the room where the symposium will be held. However, you may use them in the common areas within the SCIF Conference Center. | You did not select the correct response. Since the entire Conference Center is a SCIF, PEDS and storable media are not permitted in any area within the SCIF Conference Center and must be left outside. |
| | PEDs (e.g., cell phones, MP3 players, cameras) can be distracting. Please make sure that these devices are turned off during the symposium. | You did not select the correct response. Since the entire Conference Center is a SCIF, PEDS and storable media are not permitted in any area within |

the SCIF Conference Center and must be left outside. Turing the device off does not comply with this requirement.

Classified Discussions and Notes

The information presented at the symposium will be classified up to the TS//SI//TK level. You need to make sure that the attendees are aware of regulations concerning classified discussions and notes. If they take any classified notes, the notes will be delivered to them at their home office via classified fax. Secure fax machines accredited to the appropriate level will be used.

Review the statements below, [select the most appropriate one to put in your pre-symposium packet, and then select SUBMIT.](#)

| Correct | Choice | Feedback |
|---------|--|---|
| X | Remember that all classified discussions need to take place in the SCIF. If you take notes on the classified information that is presented, you will need to bring the phone number of a secure fax machine that is accredited to receive information classified at this level so that your notes can be faxed to you. | That's right! You selected the correct response. The symposium is going to be held at the TS//SI//TK level. This level requires that all conversations take place only in a SCIF and that all paper copies of information are controlled at this level. If classified notes are taken, they will be sent by fax machine to another one that is accredited to receive this level of information. There are other methods of transporting classified information; however, they are not available at this event. |
| | Remember that all classified discussions need to take place in the SCIF. If you take notes based on classified information, you | You did not select the correct response. The symposium is going to be held at the TS//SI//TK |

will need to place them in an envelope and seal it, so that you may take them with you when you leave.

level. This level requires that all conversations take place only in a SCIF and that all paper copies of information are controlled at this level. Taking classified notes, placing them in an envelope, and sealing it is not a sufficient means to protect the information during transportation. For this event, all classified notes will be sent by secure fax machine to another one that is accredited to receive this level of information. There are other methods of transporting classified information, however, they are not available at this event.

Compiled Welcome Letter

This letter confirms your registration for the Protecting Our Borders Symposium. The symposium will take place on June 28 from 0800-1200 at the SCIF Conference Center. This letter contains useful information and reminders about the symposium. Please let me know if you have any questions.

Facility

The symposium is taking place in a multi-room SCIF at the Conference Center. On the day of the event, you will need to bring a U.S. Government-issued photo ID (e.g., passport, drivers license, IC badge). You will not be granted access to the facility without it.

Clearances

You will need to have your TS//SI//TK clearances and accesses passed to the security office at the SCIF Conference Center. Include a "no later than" date for when the clearances are due at the SCIF. Have your SSO complete the enclosed clearance and access form and fax it to Pat at XXX-XXX-XXXX.

Portable Electronic Devices and Storable Media

PEDs (e.g., cell phones, MP3 players, cameras) and storable media (e.g. thumb drives, floppy disks, external hard drives) are not permitted in the

SCIF Conference Center at all. Please make sure that you leave them in your car.

Classified Discussions and Notes

Remember that all classified discussions need to take place in the SCIF. If you take notes on the classified information that is presented, you will need to bring the phone number of a secure fax machine that is accredited to receive information classified at this level so that your notes can be faxed to you.

Create the Classified Pre-reading Material

The symposium is just four weeks away. It is time for you to create the pre-symposium packets that will include classified pre-reading material.

Review the classified pre-reading material:

- Identify the appropriate security markings
- Validate the markings of the material for accuracy

You are going to validate the classification markings of the pre-reading material. Review the list of the following components, select the components that need to be included, and then select SUBMIT.

| Correct | Choice |
|---------|--|
| X | Banner lines (headers and footers) with the overall classification, any formal access control system markings, and dissemination control markings of the information contained in the document |
| | Portion marks for only the classified paragraphs |
| X | Portion marks for all paragraphs |
| X | Classification authority block |
| | Source information for each classified paragraph |

Feedback when correct:

That's right! You selected the correct responses.

When you create a derivative document, you need to include:

- Banner lines with the overall classification, any formal access control system markings, and dissemination control markings of the information contained in the document
- Portion marks for all paragraphs regardless of classification
- Classification authority block, which provides source information and declassification guidance

Feedback when incorrect:

You did not select the correct responses.

When you create a derivative document, you need to include:

- Banner lines with the overall classification, any formal access control system markings, and dissemination control markings of the information contained in the document
- Portion marks for all paragraphs regardless of classification
- Classification authority block, which provides source information and declassification guidance

You have identified the classification markings components that need to be included in the pre-reading material. Review the documents below, select the one that is appropriately marked, and then select SUBMIT.

| Correct | Choice | Feedback |
|---------|---------|--|
| | Flyer 1 | <p>You did not select the correct answer.</p> <p>This document is incorrect for several reasons.</p> <ul style="list-style-type: none"> • The document contains TS//HCS level information. This level of information is not appropriate for this symposium which will be held at the TS//SI//TK level. • The overall classification found in the banner lines does not match the information contained in the document. It should be marked TOP SECRET//HCS/ SI/ TK//NOFORN. |
| X | Flyer 2 | <p>That's right! You selected the correct answer.</p> <p>This document is marked</p> |

correctly.

- Portion marks are appropriate for the information contained in each portion.
- Banner lines contain the overall classification, any formal access control system markings, and dissemination control markings.
- Classification authority block contains information regarding who classified the information, the source of the information, and declassification instructions.

Congratulations!

You have just created your pre-symposium packet.

Slide 87

Congratulations – You are Done!

Your planning for the symposium was meticulous. This planning required coordination between various stakeholders and security. You were able to ensure that security regulations and policies were followed for each of the key security methods. For example:

| Personnel Security | Physical and Technical Security | Information Assurance and Cyber Security | Classification Management |
|---|--|---|---|
| <ul style="list-style-type: none"> • Provided information to the attendees for the proper passing of their clearances and accesses • Identified attendees not possessing certain accesses and coordinated escort procedures | <ul style="list-style-type: none"> • Created a plan for controlling access to the SCIF Conference Center • Established a means for transporting classified information | <ul style="list-style-type: none"> • Established a method for transferring the presentation and loading it onto the classified network | <ul style="list-style-type: none"> • Recalled the required classification markings that need to be included in the pre-reading materials • Validated that a pre-reading materials contained the appropriate classification markings |

Congratulations – You are Done!

Your planning for the symposium was meticulous. This planning required coordination between various stakeholders and security. You were able to ensure that security regulations and policies were followed for each of the key security methods. For example:

| Personnel Security | Physical and Technical Security | Information Assurance and Cyber Security | Classification Management |
|---|--|---|---|
| <ul style="list-style-type: none"> • Provided information to the attendees for the proper passing of their clearances and accesses • Identified attendees not possessing certain accesses and | <ul style="list-style-type: none"> • Created a plan for controlling access to the SCIF Conference Center • Established a means for transporting classified information | <ul style="list-style-type: none"> • Established a method for transferring the presentation and loading it onto the classified network | <ul style="list-style-type: none"> • Recalled the required classification markings that need to be included in the pre-reading materials • Validated that a pre-reading materials contained the |

| | | | |
|---|--|--|--|
| <p>coordinate d escort procedures</p> | | | <p>appropriat e classificati on markings</p> |
|---|--|--|--|

Slide 88



Course Summary

Congratulations! You have just completed the *IC Security Today* course in which you had the opportunity to review and apply security concepts. Remember, security policies and procedures are in place to protect our nation's greatest secrets; secrets with which you have been entrusted.

To keep these secrets safe, it is important that you maintain security awareness in both your personal and professional lives.

- Be cognizant of information you share about your professional life with others
- Report any and all security incidents (remember, when in doubt, report)
- Follow all security policies and procedures
- Ask your SSO and/or supervisor for guidance whenever you are in doubt

Please continue to the next slide for additional information about your Certificate of Completion.

(Alt Image: Pat standing in front of the American flag).