Student Guide

Course: Sensitive Compartmented Information (SCI) Refresher

Lesson 1: Course Introduction

Course Information

Purpose	Provide annual refresher training on how to protect Sensitive Compartmented Information (SCI) and Sensitive Compartmented Information Facilities (SCIFs)
Audience	Military, civilian, and contractor personnel who work in a Sensitive Compartmented Information Facility (SCIF), including those who are responsible for the security of a SCIF, namely the Special Security Officers (SSOs) and Special Security Representatives (SSRs)
Pass/Fail %	75% on final examination
Estimated completion time	120 minutes

Course Overview

Because the United States Government has placed its trust in you, you have been given access to SCI. Whether you've had access to SCI for a long time or just received it in the past year, you know that when you protect SCI, you are protecting our nation's security along with the war fighters defending the American way of life.

In this course, you will review who in the Intelligence Community works with SCI, what intelligence collection methods are used to gather SCI, and what your responsibilities are, as outlined in your SCI Nondisclosure Statement, to protect SCI both inside and outside your Sensitive Compartmented Information Facility (SCIF).

In addition, throughout this course you will occasionally see information that is specific to the Special Security Officer (SSO) and Special Security Representative (SSR) roles. When you see this content, only SSOs and SSRs are required to review the associated information. All others may bypass this information.

Course Objectives

Here are the general course objectives:

- Recognize SCI policy guidance documents
- Identify the purpose and components of the Sensitive Compartmented Information (SCI) Nondisclosure Statement (NdS)
- Apply classification markings and dissemination controls for SCI materials
- Identify the proper methods for handling, discussing, reproducing, transporting, and destroying SCI material
- Identify the proper procedures for visitors and escorts in a SCIF
- List the types of accredited SCIFs and their purposes
- Recognize the types of information that must be reported by or about individuals who have SCI access

Here are additional course objectives for SSOs/SSRs:

- Identify the process for SCI pre-screening and indoctrination
- Identify the SCIF accreditation process
- Identify the components of the Fixed Facility Checklist (FFC)

Course Structure

This course is organized into the following lessons:

- Course Introduction
- SCI Fundamentals
- SCI Control Systems and Markings
- Protecting SCI
- SCI Reporting Requirements
- Course Conclusion

Student Guide

Course: Sensitive Compartmented Information (SCI) Refresher

Lesson 2: SCI Fundamentals

Lesson Introduction

1. Opening

Our democratic principles require that the American people be informed of the activities of their Government. Also, our nation's progress depends on the free flow of information.

Nevertheless, throughout our history, the national interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. Executive Order 13526 states, in part: "…the national interest has required that certain information be maintained in confidence in order to protect…"

Through the use of controlled environments, classification, and compartmentation, we protect our assets and our nation's security from threats such as spies, insiders, terrorists, and foreign intelligence services.

Your position exposes you to Sensitive Compartmented Information emanating from the Intelligence Community. SCI involves intelligence sources and methods that are the Intelligence Community's most treasured secrets. Although the protection challenge is significant, **it is your life-long security responsibility and legal obligation to protect SCI.**

2. Objectives

In this lesson, you will review fundamental information about SCI such as the members of the Intelligence Community (IC), SCI policy and guidance documents, and the SCI Nondisclosure Statement.

Here are the lesson objectives:

- Recognize SCI policy and guidance documents
- Identify the purpose and components of the SCI Nondisclosure Statement

3. IC Members

As you are aware, SCI is generated and regulated by various entities within the U.S. Intelligence Community (IC). The IC is headed by the Director of National Intelligence (DNI) and comprises the Central Intelligence Agency (CIA), which is an independent agency, as well as Departmental Intelligence Elements, which are government agencies, and Department of Defense (DOD) Intelligence Elements, which are the defense agencies and military components.

The DNI and the Defense Intelligence Agency (DIA) have direct authority over Sensitive Compartmented Information Facilities (SCIFs) in that the DNI establishes the security requirements for SCIFs and the DIA is responsible for the accreditation of DOD SCIFs.

Intelligence Community – Review Activity

Who provides governance for SCIFs? *For each question, select the best answer. Then check your answers in the Answer Key at the end of this Student Guide.*

1) Who provides construction and security requirements for SCIFs?

   - ○ Director of National Intelligence (DNI)
   - ○ Central Intelligence Agency (CIA)
   - ○ Defense Intelligence Agency (DIA)
   - ○ Department of Defense (DOD)

2) Who provides accreditation for DOD SCIFs?

   - ○ Director of National Intelligence (DNI)
   - ○ Central Intelligence Agency (CIA)
   - ○ Defense Intelligence Agency (DIA)
   - ○ Department of Defense (DOD)

SCI Policy and Guidance Documents

1. Guidance Overview

Let's look at a brief overview of the policies that guide your actions in protecting Sensitive Compartmented Information.

In 1981, the President issued Executive Order 12333, United States Intelligence Activities, which established the role of Senior Officials of the Intelligence Community (SOICs) and designated the DNI as the head of the IC for intelligence matters related to national security.

In 2008, the President issued Executive Order 13470, further amendment to Executive Order 12333, which changed the SOIC role to Head of an Intelligence Community Element, or HICE. Subsequently, the DNI issued several Intelligence Community Directives (ICDs) and Intelligence Community Policy Guidance documents (ICPGs) which provide security policy for the protection of national intelligence as well as the personnel security requirements for access to SCI and SCIFs and physical and technical security requirements for SCIFs.

To see the ICDs or ICPGs, you may visit http://www.dni.gov/index.php/ncsc-how-we-work/ncsc-ci-security-governance-regulations In addition, the DOD issued guidance that prescribes security policy and procedures for the protection, use, and dissemination of SCI within DOD SCIFs.

2. Job Aids

Originator: Executive Branch

Key Guidance Documentation	Description
Executive Order (EO) 12333 ***United States Intelligence Activities*** 4 Dec 1981, as amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)	This order established the Senior Officials of the Intelligence Community (SOICs), now referred to as HICE per E.O. 13470, as the authority within their military departments or agencies to protect intelligence and intelligence sources and methods and designated the Director of National Intelligence (DNI) as the head of the Intelligence Community for intelligence matters related to national security.

Originator: Department of Defense (DOD)

Key Guidance Documentation	Description
DODI 5200.01 Incorporating Change 1 ***DOD Information Security Program and Protection of Sensitive Compartmented Information*** 9 Oct 2008 Incorporating Change 1, June 13, 2011	This instruction updated policy and assigned responsibilities to DIA to inspect and accredit DOD SCIFs for the handling, processing, storage, and discussion of SCI.
DODM 5105.21, Volume 1 ***Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Information and Information Systems Security*** 19 October 2012 **DOD Manual 5105.21, Volume 2** ***Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security*** 19 October 2012 **DOD Manual 5105.21, Volume 3** ***Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities*** 19 October 2012	This Manual is composed of several volumes, each containing its own purpose, and reissues DOD Manual 5105.21-M-1. The purpose of the overall Manual, in accordance with the authority in DOD Directive 5143.01, is to implement policy established in DOD Instruction 5200.01, and Director of Central Intelligence Directive 6/1 for the execution and administration of the DOD SCI program. It assigns responsibilities and prescribes procedures for the implementation of Director of Central Intelligence and Director of National Intelligence (DNI) policies for SCI.

Originator: Intelligence Community (IC)

Key Guidance Documentation	Description
ICD 700 ***Protection of National Intelligence*** 21 Sep 2007	This guidance established the DNI security policy to protect national intelligence, and DNI's responsibilities for oversight and direction of IC security programs and activities. It also described the roles and responsibilities of the Senior Officials of the Intelligence Community (SOICs), now referred to as HICE per E.O. 13470.

Key Guidance Documentation	Description
ICD 704 ***Personnel Security (previously DCID 6/4)*** 1 October 2008	This guidance established the DNI personnel security policy governing eligibility for access to SCI and information protected within other Controlled Access Programs.
ICPG 704.1 ***Personnel Security Investigative Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*** 2 October 2008	This guidance established the investigative standards used to conduct National Agency Check with Law and Credit (NACLC), Single Scope Background Investigations (SSBI), and periodic reinvestigations (PR) for access to SCI and information protected within other Controlled Access Programs.
ICPG 704.2 ***Personnel Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information*** 2 October 2008	This guidance established the adjudicative guidelines used in determining one's eligibility for access to SCI and information protected within other Controlled Access Programs.
ICPG 704.3 ***Denial or Revocation of Access to Sensitive Compartmented Information, Other Controlled Access Program Information, and Appeals Processes*** 2 October 2008	This guidance established the process one may go through to appeal the denial or revocation of access to SCI and information protected within other Controlled Access Programs.
ICPG 704.4 ***Reciprocity of Personnel Security Clearance and Access Determinations*** 2 October 2008	This guidance established that heads of IC elements must accept investigations, security clearances and access determinations made by other IC elements within the past seven years as the basis for initial or continuing access to SCI or information protected within other Controlled Access Programs.
ICPG 704.5 ***Intelligence Community Personnel Security Database Scattered Castles*** 2 October 2008	This guidance mandated the recognition and use of the Scattered Castles (SC) database, or successor database, as the IC's authoritative personnel security repository for verifying personnel security access approvals regarding SCI and other Controlled Access Programs, visit certifications, and documented exceptions to personnel security standards.

Key Guidance Documentation	Description
ICD 705 ***Sensitive Compartmented Information Facilities*** 26 May 2010	This Directive establishes that all Intelligence Community (IC) Sensitive Compartmented Information Facilities (SCIF) shall comply with uniform IC physical and technical security requirements (hereafter "uniform security requirements"). This Directive is designed to ensure reciprocal use of SCIFs in the IC. This Directive applies to all facilities accredited by IC elements where SCI is processed, stored, used, or discussed.
ICD 705-1 ***Physical and Technical Security Standards for Sensitive Compartmented Facilities*** 17 Sep 2010	This Intelligence Community Standard sets forth the physical and technical security standards that apply to all Sensitive Compartmented Information Facilities (SCIF), including existing and new construction, and renovation of SCIFs for reciprocal use by all IC elements and to enable information sharing to the greatest extent possible. This standard facilitates the protection of SCI, including protection against compromising emanations, inadvertent observation or overhearing, disclosure by unauthorized persons, forced entry, and the detection of surreptitious and covert entry. The Assistant Deputy Director of National Intelligence for Security (ADDNI/SEC) shall consult with IC elements, develop and establish technical specifications to implement SCIF standards that include descriptions of best practices, and review and update the IC Tech Spec on an ongoing basis.
ICS 705-2 ***Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Information Facilities*** 17 Sep 2010	This Intelligence Community Standard sets forth the criteria that apply to the accreditation of Sensitive Compartmented Information Facilities (SCIF) to enable reciprocal use by Intelligence Community (IC) elements and to facilitate information sharing to the greatest extent possible.
IC Tech Spec – for ICD/ICS 705 ***Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities*** 5 May 2011	Sets forth the physical and technical security specifications and best practices for meeting standards of ICS 705-1. This document is the implementing specification for ICD 705 and ICS 705-2 and supersedes DCID 6/9.

SCI Nondisclosure Statement

1. Purpose

As you will recall, in order to work in a SCIF and have access to SCI, you went through a pre-screening process with an SSO or SSR. Once approved for SCI access, you went through an indoctrination process with the SSO or SSR during which you were required to sign an SCI Nondisclosure Statement (NdS). The SCI NdS is a contract between you and the U.S. Government in which you made a lifelong commitment to protect U.S. Government classified intelligence information. In just a moment, we'll review the NdS that you signed in more detail.

SSOs and SSRs should take a moment to review the steps of the pre-screening and indoctrination processes below.

NOTE: The information in the box below is provided for the benefit of SSOs and SSRs. For additional information on investigations and adjudications, refer to the Personnel Security web-based training course offered by the DSS Center for Development of Security Excellence.

Pre-Screening Process
Guidelines for conducting personal screening interviews: 1. Prepare for interview by reviewing individual's records and investigative forms. 2. Understand that questions you ask must be relevant to security determination. 3. Advise individual 4. About the purpose of the interview a. That you are not affiliated with any investigative or law enforcement agency b. That he/she is not suspected of any wrongdoing c. That interview is voluntary d. Have individual sign the SCI Pre-Screening Interview acknowledgement. 5. Provide individual Privacy Act Advisement. 6. Ask Pre-Screening Interview questions. 7. Offer individual opportunity to provide additional information. 8. In personnel security files, keep justifications for SCI access and approvals or disapprovals for two years after accountability ceases; does not apply to contractors.

NOTE: The information in the box below is provided for the benefit of SSOs and SSRs. Indoctrination is the instructions an individual receives prior to receiving access to an SCI system or program. The instructions convey the unique nature, unusual sensitivity, and special security safeguards and practices for SCI handling, particularly the necessity to protect sensitive sources and methods.

Indoctrination Process

Guidelines for conducting indoctrinations:

1. Provide individual Pre-Nondisclosure Execution briefing on protecting SCI.
2. Have individual read E.O. 13526 and the SCI Nondisclosure Statement (NdS), DD Form 1847-1.
3. Provide individual opportunity to express any reservations concerning the execution of the SCI NdS.
4. If no reservations, have individual complete the SCI NdS and sign it in front of a witness, who also signs it.
5. The SCI NdS must be accepted for the Government by a military member, Government civilian personnel, and by contractors, consultants, or non-government personnel.
6. Classify the SCI NdS, as required.
7. Provide copy of the SCI NdS to individual, if requested. Populate the NdS date in JPAS on the date it was signed by the individual. The Investigative Records Repository, IAMG-CICIRRH, 4552 Pike Road, Fort Meade, MD 20755 is responsible for retaining in a retrievable manner the original NdS for at least 70 years or until death of the individual.
8. Indoctrinate individual on SCI access; show approved Indoctrination videos for the appropriate SCI compartments.
9. Have individual sign an Indoctrination Memorandum, DD Form 1847.

Note: Once a HICE has determined that an individual is ICD 704 eligible without waiver and is currently briefed into at least one SCI program, the individual may be approved for additional accesses by any Senior Intelligence Officer (SIO) without further security adjudication.

2. Details

Now let's review the details of the SCI NdS that you signed.

Sensitive Compartmented Information Nondisclosure Statement

Purpose: *Lifelong commitment from you to protect U.S.G. classified intelligence information.*

Paragraph 1	Accepting agreement to protect SCI	You accepted the agreement to protect SCI and understand that a special confidence and trust was placed in you by the U.S. Government.
Paragraph 2	Acknowledging SCI Indoctrination	You acknowledged that you received a security indoctrination concerning the nature and protection of SCI, including the procedures to be followed regarding disclosure of SCI information.

Sensitive Compartmented Information Nondisclosure Statement		
Paragraph 3	Avoiding unauthorized disclosures	You acknowledged that you were advised that mishandling SCI could cause irreparable harm to the United States and you are obligated not to disclose SCI to anyone who is not authorized to receive it.
Paragraph 4	Public release requirements	You agreed to submit for security review to the department or agency that last authorized your SCI access any information you prepare for public disclosure that contains or might contain or relate to SCI.
Paragraph 5	30-day Government response	You acknowledged that you must allow the department or agency to have up to 30 days to approve or deny your request for public disclosure.
Paragraph 6	Consequences of breach of agreement	You acknowledged that any breach of this Statement might result in the termination of your SCI access and your employment as well as prosecution of you under the U.S. criminal laws.
Paragraph 7	Government action for breach of agreement	You acknowledged that the U.S. Government might seek any remedy available to enforce this agreement including bringing action against you in which you would be responsible for court costs and attorneys' fees if you lost such action.
Paragraph 8	SCI is USG property	You acknowledged that SCI is and always will be the property of the U.S. Government.
Paragraph 9	Agreement is forever	You acknowledged that this agreement will last forever, unless you are released in writing by an authorized representative of the department or agency that last granted you with access to SCI.
Paragraph 10	Severable provisions in agreement	You acknowledged that there are severable provisions in this agreement but that if a court should find any provision of this agreement to be unenforceable, all other provisions of this agreement will remain in full force.
Paragraph 11	Whistleblower protection	You acknowledged that there are laws and statutes that protect you such as the Whistleblowers Protection Act that do not conflict with this agreement.

Sensitive Compartmented Information Nondisclosure Statement		
Paragraph 12	Laws protecting national security information	You acknowledged that you read this agreement, that your questions were answered, and that the laws and statutes referenced in paragraph 12 were made available to you to read, if you wished to read them.
Paragraph 13	Fate of ill gotten gains	You agreed that anything you gained from unauthorized disclosure of SCI would become the property of the United States Government.
Paragraph 14	Agreement in conformance with U.S. Law	You acknowledged that this agreement is in conformance with U.S. laws.
Paragraph 15	Signing agreement without mental reservation	You acknowledged that you made this agreement without any mental reservation or purpose of evasion.

The SCI NdS that you signed is retained in your personnel security file along with several other documents.

SSOs and SSRs should take a moment to review what must be retained for an individual who has had or has access to SCI.

NOTE: The information in the box below is provided for the benefit of SSOs and SSRs.

Personnel Security Files

SSOs are required to maintain certain information in personnel security files for each SCI-indoctrinated person.

- Valid ICD 704 authority
- SCI indoctrination information
- SCI debrief
- DD Form 1847-1
- Other security personnel action or defensive security briefings and memoranda
- Reports: derogatory information/changes in personal status
- Reports: personal screening interview/foreign travel and contacts
- Justifications for SCI access: approvals/ disapprovals

All but the last item shown here are to be maintained during the individual's assignment and for a minimum of 180 days after accountability of the individual ceases. Justifications for SCI access and approvals or disapprovals must be maintained in the personnel security files for two years after an individual's accountability ceases. However, this requirement does not apply to contractors.

3. Termination of SCI Access

An individual will be denied further access to SCI when the need-to-know for SCI access has ceased, an individual's access to SCI is terminated for cause, an individual retires or separates from the Federal Government, or an individual dies. The responsibility for terminating access to SCI rests with the HICE or designee who granted the access. The SSO is responsible for accomplishing and reporting the debrief action and canceling all current visitor certifications pertaining to the debriefed individual.

A Head of an Intelligence Community element (HICE) is the head of an agency, organization, bureau, office, intelligence element, or activity within the IC, as defined in Section 3 of the National Security Act of 1947, as amended, and Executive Order 12333, as amended by 13470 signed 30 Jul 2008.

SSOs and SSRs should take a moment to review the steps they must perform.

NOTE: The information in the box below is provided for the benefit of SSOs and SSRs.

Debriefing Process
Guidelines for debriefing 1. Have the individual read the appropriate sections of Titles 18 and 50 of the United States Code (USC). 2. Provide the individual a statement emphasizing the requirement for continued security for SCI. 3. Have the individual provide an acknowledgement that he/she will report without delay to the FBI, or the department or agency, any attempt by an unauthorized person to solicit national security information. 4. Remind the individual about the risks associated with foreign travel and the department or agency reporting requirements. 5. Have the individual sign the Debriefing Memorandum.

SCI Nondisclosure Statement – Review Activity 1

Which of the following statements are true about the SCI NdS and having access to SCI? *Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.*

You are required to submit for security review to the department or agency that last authorized your SCI access any information you prepare for public disclosure that contains or might contain or relate to SCI.

- True
- False

If a court should find any provision of the SCI NdS to be unenforceable, then all other provisions of the agreement will be unenforceable.

- True
- False

The SCI agreement will last forever, unless you are released in writing by an authorized representative of the department or agency that last granted you with access to SCI.

- True
- False

SCI Nondisclosure Statement – Review Activity 2

Which of these statements are true about the SCI NdS and having access to SCI? *Select True or False for each statement. Then check your answers in the Answer Key at the end of this Student Guide.*

When you are authorized access to SCI, the U.S. Government places a special confidence and trust in you.

- True
- False

Any breach of the SCI NdS could result in the termination of your SCI access and your employment as well as prosecution of you under the U.S. criminal laws.

- True
- False

Answer Key

Intelligence Community – Review Activity

Who provides governance for SCIFs?

1) Who provides construction and security requirements for SCIFs?

    - ⦿ Director of National Intelligence (DNI) (correct)
    - ○ Central Intelligence Agency (CIA)
    - ○ Defense Intelligence Agency (DIA)
    - ○ Department of Defense (DOD)

Feedback: The Director of National Intelligence (DNI) provides the construction and security requirements for SCIFs.

2) Who provides accreditation for DOD SCIFs?

    - ○ Director of National Intelligence (DNI)
    - ○ Central Intelligence Agency (CIA)
    - ⦿ Defense Intelligence Agency (DIA) (correct)
    - ○ Department of Defense (DOD

Feedback: The Defense Intelligence Agency (DIA) provides accreditation for DOD SCIFs.

SCI Nondisclosure Statement – Review Activity 1

Which of the following statements are true about the SCI NdS and having access to SCI?

You are required to submit for security review to the department or agency that last authorized your SCI access any information you prepare for public disclosure that contains or might contain or relate to SCI.

- True (correct)
- ○ False

Feedback: In paragraph 4 of the SCI NdS, you agreed to submit for security review to the department or agency that last authorized your SCI access any information you prepare for public disclosure that contains or might contain or relate to SCI.

If a court should find any provision of the SCI NdS to be unenforceable, then all other provisions of the agreement will be unenforceable.

- ○ True
- False (correct)

Feedback: In paragraph 10 of the SCI NdS, you acknowledged that there are severable provisions in the agreement but that if a court should find any provision of the agreement to be unenforceable, all other provisions of the agreement would remain in full force.

The SCI agreement will last forever, unless you are released in writing by an authorized representative of the department or agency that last granted you with access to SCI.

- True (correct)
- False

Feedback: In paragraph 9, you acknowledged that the agreement will last forever, unless you are released in writing by an authorized representative of the department or agency that last granted you with access to SCI.

SCI Nondisclosure Statement – Review Activity 2

Which of the following statements are true about the SCI NdS and having access to SCI? Select True or False for each statement.

When you are authorized access to SCI, the U.S. Government places a special confidence and trust in you.

- True (correct)
- False

Feedback: In paragraph 1, you accepted the agreement to protect SCI and understood that a special confidence and trust was placed in you by the U.S. Government.

Any breach of the SCI NdS could result in the termination of your SCI access and your employment as well as prosecution of you under the U.S. criminal laws.

- True (correct)
- False

Feedback: In paragraph 6, you acknowledged that any breach of the agreement might result in the termination of your SCI access and your employment as well as prosecution of you under the U.S. criminal laws.

Student Guide

Course: Sensitive Compartmented Information (SCI) Refresher

Lesson 3: SCI Control Systems and Markings

Lesson Introduction

1. Objectives

As you know, additional protection is provided to Sensitive Compartmented Information (SCI) through classification management and marking, above and beyond what is provided to classified information. In this lesson, you will review what classification management is and how intelligence is collected and then protected with SCI control systems and markings. This lesson also provides an overview of the SCI management tools you may use in your daily work with SCI.

Here is the lesson objective:

- Identify classification markings and dissemination controls for SCI materials

Classification Management

Overview

We use classification management to determine the nature of information and assign proper classification markings, SCI control system markings, dissemination controls, and the contents of the classification authority block.

2. What Information is Protected as Classified

Executive Order (E.O.) 13526 outlines eight categories of information that require classified protection:

1.4(a) Military plans, weapons systems or operations
1.4(b) Foreign government information
1.4(c) Intelligence activities (including covert action), intelligence sources and methods or cryptology
1.4(d) Foreign relations or activities of the US, including confidential sources
1.4(e) Scientific, technological or economic matters relating to national security
1.4(f) Program for safeguarding nuclear materials or facilities
1.4(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects/plans relating to national security
1.4(h) Weapons of mass destruction

Classified national intelligence information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems, is the information we call SCI.

3. How Intelligence Information is Collected

As you know, there are six basic intelligence sources or collection disciplines that gather intelligence using human sources such as diplomats or military attaches:

- Through public sources such as the press and media
- Via verbal and nonverbal signals from land, sea, and satellite
- Using geographical references through imagery, mapping, satellites, and aircraft
- By locating, identifying, and describing distinctive characteristics of targets
- From visual photography, radar sensors, or electro-optics

a. Human Intelligence (HUMINT)

HUMINT, or Human Intelligence, is the collection of intelligence using human sources such as diplomats, military attachés, and even spies. This was the primary source before technical revolution. Methods include collection of photography, documents, and other material, debriefing of foreign nationals and U.S. citizens who travel abroad, and official contact with foreign governments. The CIA, DOD, Department of State, and FBI use HUMINT.

b. Open-Source Intelligence (OSINT)

OSINT, or Open-Source Intelligence, is the collection of intelligence through public sources. OSINT is broadly distributed throughout the IC. Major collectors of OSINT include the DNI's Open Source Center (OSC) and the National Air and Space Intelligence Center.

OSINT sources include:

- Press/media
- Internet
- Speeches
- Articles
- Libraries
- Symposiums
- Conferences
- Commercial databases
- Videos
- Graphics
- Drawings
- Social media

c. Signals Intelligence (SIGINT)

SIGINT, or Signals Intelligence, is the collection of verbal and nonverbal signals from land, sea, and satellite. These signals are protected within the Communications Intelligence (COMINT) SCI control system. Categories of SIGINT include COMINT, Electronic Intelligence (ELINT), and Foreign Instrumentation Signals (FISINT). The National Security Agency (NSA) is responsible for the collecting, processing, and reporting of SIGINT.

d. Geospatial Intelligence (GEOINT)

GEOINT, or Geospatial Intelligence, uses imagery, imagery intelligence, or geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the earth. GEOINT enhances the situational awareness of policy makers, military planners, and military operators. The National Geospatial Intelligence Agency (NGA) is responsible for the collecting, processing, and reporting of GEOINT.

e. Measurement and Signature Intelligence (MASINT)

MASINT, or Measurement and Signature Intelligence, is technically derived intelligence data other than imagery and signals intelligence. Data results in intelligence that locates, identifies, or describes distinctive characteristics of targets. Examples of MASINT are distinctive radar signatures of specific aircraft systems and chemical composition of air and water samples. The Defense Intelligence Agency (DIA) is responsible for the collecting, processing, and reporting of MASINT. MASINT includes the following sciences:

- Nuclear
- Optical
- Radio frequency
- Acoustics
- Seismic
- Material

f. Imagery Intelligence (IMINT)

IMINT, or Imagery Intelligence, includes representations of objects reproduced electronically or by optical means on film, electronic display devices, or other media. IMINT is derived from visual photography, radar sensors, and electro-optics. The NGA is responsible for the collecting, processing, exploitation, dissemination, archiving, and retrieval of IMINT.

SCI Control Systems

Overview

SCI control systems are additional measures used to protect intelligence sources and methods or analytical procedures that are beyond those used to protect non-SCI classified information.

Types

The current SCI control systems are:

- HCS is the marking for Human Intelligence which replaced HUMINT
- SI is the marking for Special Intelligence and replaced COMINT, which has:
  - A sub-control system of GAMMA
- TALENT KEYHOLE
- KDK is the marking for KLONDIKE.
- In addition, there are three legacy SCI control systems you may still encounter: BYEMAN, HUMINT, and COMINT.

For recent changes to SCI control systems, reference the Joint Worldwide Intelligence Communications System (JWICS).

Anatomy of a Classified Document

Overview

Take a moment to review the hierarchy of classification markings found in the banner line on the top and bottom of a classified document.

1. U.S. Classification, Non-U.S. Classification, Joint Classification
2. SCI Control System, Special Access Program
3. AEA
4. Foreign Government Information Markings
5. Dissemination Controls
6. Non-Intelligence Communication Markings

Here is the format for how these markings appear on a classified document.

CLASSIFICATION//SCI//SAP//AEA//FGI//Dissemination//Non-IC//

Here is an example of classification markings in the appropriate format.

TOP SECRET//TK//SAR-REDHAT//RD-CNWDI//FGI GBR//REL TO USA, GBR//SPECAT//

NOTE: Not all fields may be required or combined.

These markings show that the classified document is TOP SECRET, is part of the TALENT KEYHOLE SCI control system, is part of the REDHAT Special Access Program, contains Atomic Energy information, is furnished to the United States by Great Britain, is releasable only to the United States and Great Britain, and has a non-Intelligence Community marking of Special Category.

SCI Classification Markings	
U.S. Classification	U.S. Classification markings are used on U.S. classified materials that represent the amount of damage that could be caused to U.S. national security if disclosed to an unauthorized person. U.S. Classification Markings are: • TOP SECRET • SECRET • CONFIDENTIAL • UNCLASSIFIED

SCI Classification Markings	
Non-U.S. Classification	Non-U.S. Classification markings are used on documents consisting entirely of foreign information provided by other countries and international organizations. These markings must be preceded by the foreign country trigraph or foreign organization tetragraph. Non-U.S. Classification Markings are: • TOP SECRET • SECRET • CONFIDENTIAL • RESTRICTED • UNCLASSIFIED *Example of foreign country non-U.S. classification marking:* • //DEU CONFIDENTIAL *Example of foreign organization non-U.S. classification marking:* • //NATO SECRET
Joint Classification	Joint Classification markings are used on information that is jointly owned and/or produced by more than one country and/or international organization. *Example of Joint Classification marking:* • //JOINT SECRET CAN GBR USA
SCI Control System	SCI Control System markings indicate to which SCI Control System the information belongs.
Special Access Program	Special Access Program markings denote classified information that requires extraordinary protection as allowed by E.O. 13526, as amended.
Foreign Government Information Markings	Foreign Government Information markings are used to indicate that foreign government information is included in U.S. produced documents. Use the foreign country trigraph after FGI.
Dissemination Controls	Dissemination controls are used to indicate to whom information may be released.
Non-Intelligence Community Markings	Non-Intelligence Community markings are used by entities outside of the IC.
AEA	Atomic Energy Act (AEA) information markings are used in US products to denote the presence of classified Restricted Data, Formerly Restricted Data, and/or Transclassified Foreign Nuclear Information (TFNI). Must have RD Warning and CNWDI Statement when used.

SCI Control System Markings

As you know, there are several SCI control system markings that correspond to the SCI control systems you just reviewed. Some SCI control system markings are currently in use and some are legacy SCI control system markings that you may still see on older SCI documents.

SCI Control System Marking (Current)	
HCS	HCS is the SCI control system marking that corresponds to the HCS SCI control system which is designed to protect human intelligence.
KDK	The KLONDIKE control system is a sensitive compartmented information (SCI) control system designed to protect sensitive Geospatial Intelligence (GEOINT).
SI	SI is designed to protect signals intelligence including communications and electronics intelligence. It was formerly named for the first product it afforded protection, which was COMINT (Communications Intelligence). Now it is called the Special Intelligence (SI) Control System. SI information is only available to holders of SI access approval and is managed by the Director of the National Security Agency (D/NSA).
G	G is an SCI control system marking that corresponds to the GAMMA SCI sub-control system.
TK	TK is the SCI control system marking that corresponds to the TALENT KEYHOLE SCI control system. TALENT KEYHOLE was established by the Director of Central Intelligence (DCI) for products from satellite reconnaissance in 1960. TK protects the most sensitive details of satellite collection capabilities and derived information. The Director of National Intelligence (DNI) has administrative oversight of the TK control system. Information within the TK compartment is managed by the originating agency. Possible originating agencies are NSA, NRO, NGA, CIA, and DIA.

SCI Control System Marking (Legacy)	
BYE	BYE is the SCI control system marking that corresponds to the BYEMAN SCI control system. The BYEMAN control system was retired on 20 May 2005. The word BYEMAN and the trigraph BYE are unclassified. All previous data protected in the BYE control system, except BYE Special Handling, will be protected in the TALENT KEYHOLE (TK) control system. BYE Special Handling is now protected in compartments in the new NRO control system, RESERVE.
HUMINT	HUMINT was registered as the marking title for the HUMINT SCI control system. Since then, there has been confusion between collateral HUMINT and HUMINT in the SCI category. So HUMINT was retired as an SCI category. When creating new documents, if HUMINT is present in the SCI category, change it to HCS.

COMINT	The COMINT title for the Special Intelligence (SI) control system is no longer valid. All references to the Special Intelligence control system shall be made using the SI marking. IC elements have up to one year from the publication date of the CAPCO Register, v4.2 to incorporate this change in automated systems.

Dissemination Control Markings

In addition to SCI control system markings, there are several dissemination control markings created for use on SCI material.

Dissemination Control Marking Abbreviation	Dissemination Control Marking Title	Marking Sponsor
RSEN	Risk Sensitive	NGA
CUI	Controlled Unclassified Information	Various agencies
ORCON	Originator Controlled	DNI
IMCON	Controlled Imagery	DNI
NOFORN	Not Releasable to Foreign Nationals	DNI; all HCS material requires this
PROPIN	Caution – Proprietary Information Involved	DNI
REL TO _____	Authorized for Release to	DNI
RELIDO	Releasable by Information Disclosure Official	DNI
n/a	USA/ ___EYES ONLY	NSA/NSG
n/a	DEA SENSITIVE	DEA
FISA	Foreign Intelligence Surveillance Act	DNI
n/a	DISPLAY ONLY	DNI

Anatomy of a Classified Document – Review Activity

You've received a document today that is TOP SECRET, is part of the COMINT control system, and may not be shared with other countries. Select the appropriate classification markings to show how each section of this document would be marked when you received it. Then check your answers in the Answer Key at the end of this Student Guide.

_____ // _____ // _____

Which marking belongs in the top left section?

- o TOP SECRET
- o TK
- o SI
- o REL TO USA
- o HAS
- o PROPIN
- o NOFORN
- o SECRET

Which marking belongs in the top center section?

- o TOP SECRET
- o TK
- o SI
- o REL TO USA
- o HAS
- o PROPIN
- o NOFORN
- o SECRET

Which marking belongs in the top right section?

- o TOP SECRET
- o TK
- o SI
- o REL TO USA
- o HAS
- o PROPIN
- o NOFORN
- o SECRET

Job Aid: Sources for Marking Guidance

This table provides a list of guidance sources for marking classified documents.

Source	Guidance	Web site	Description
Controlled Access Program Coordination Office (CAPCO)	(U) Intelligence Community Authorized Classification and Control Markings Register and Manual, Volume 5, Edition 1 (Version 5.1) (Effective: 30 December 2011) Administrative Update, 30 March 2012	INTELINK: capco.dssc.ic.gov INTELINK-TS: http://www.intelink.ic.gov/sites/dnissc/capco INTELINK-S: http://www.intelink.sgov.gov/sites/ssc/capco SIPRNET: capco.dss.sgov.gov	Comprehensive listing of classification markings
National Archives & Records Administration (NARA), Information Security Oversight Office (ISOO)	Marking Booklet	www.archives.gov/isoo	Guidelines for how to mark a classified document

Job Aid: SCI Management Tools

This is a summary of the SCI management tools that will help you in your day-to-day work with SCI. Take a moment to review this table.

Acronym	Full Name	How to Access	Description
JWICS	Joint Worldwide Intelligence Communications System	For access to JWICS, contact your Information Management Office (IMO).	JWICS is a 24 hour a day network designed to meet the requirements for secure (TS/SCI) multi-media intelligence communications worldwide.
JPAS	Joint Personnel Adjudication System	https://jpasapp.dmdc.osd.mil/JPAS/JPASDisclosure	The centralized DoD database of standardized personnel security processes; it virtually consolidates the DoD Central Adjudication Facilities by offering real time information concerning clearances, access, and investigative statuses to authorized DoD security personnel and other interfacing organizations (e.g., Defense Security Service, Defense Manpower Data Center, Defense Civilian Personnel Management System, Office of Personnel Management, and the Air Force Personnel Center).
SC	Scattered Castles	Access from JWICS under the Joint Dissemination System webpage: https://clearances.cia.ic.gov	The IC security clearance repository and the Director of National Intelligence's authoritative source for clearance and access information for all IC, military services, DoD civilians, and contractor personnel. DoD information is furnished by JPAS. *For use by SSO/SSR.*

Acronym	Full Name	How to Access	Description
CAB	Compartmented Address Book	Access from JWICS: /ismapp3.dia.ic.gov:444/pls/jds/jds_sec.validate_USER?=USERID=GUEST&SUBMIT=SUBMIT	A book listing the message addresses and DCS addressees of all organizations authorized to receive SCI materials. *For use by SSO/SSR.*
DCS	Defense Courier Service	Access from JWICS under the Joint Dissemination System webpage (must be registered to access this site) https://lsotools.wpafb.af.mil/dc-atcmd/index.cfm	The Defense Courier Service (DCS) is responsible for the secure and expeditious worldwide movement of highly classified, time-sensitive national security materials integral to the national command authorities' C3I systems in a selectively manned, joint DoD Command. The DCS directly supports the President, Unified and Specified CINCs, joint military operations, the Joint Chiefs of Staff, NSA, CIA, U.S. allies, Department of State, and other federal agencies.
DCAMS	Defense Courier Automated Management System	For more information on DCAMS and its usage go to: http://www.dcs.ftmeade.army.mil or contact 301.677.3786.	The DCS computer system supporting administrative and operational functions of the worldwide DCS system.
FSD	Full Service Directory	For more information on The Full Service Directory go to: https://fsdiis2.fsdreg.army.ic.gov	All of the Intelligence Community shall support and share one secure, logical IC common Full Service Directory to identify and locate individuals, organizations, and services, including associated descriptive information over TS SCI networks.

Answer Key

Anatomy of a Classified Document – Review Activity

You've received a document today that is TOP SECRET, is part of the COMINT control system, and may not be shared with other countries. Select the appropriate classification markings to show how this document would be marked when you received it.

TOP SECRET // SI // NOFORN

Which marking belongs in the top left section?

- TOP SECRET (correct)
- TK
- SI
- REL TO USA
- HAS
- PROPIN
- NOFORN
- SECRET

Which marking belongs in the top center section?

- TOP SECRET
- TK
- SI (correct)
- REL TO USA
- HAS
- PROPIN
- NOFORN
- SECRET

Which marking belongs in the top right section?

- TOP SECRET
- TK
- SI
- REL TO USA
- HAS
- PROPIN
- NOFORN (correct)
- SECRET

Student Guide

Course: Sensitive Compartmented Information (SCI) Refresher

Lesson 4: Protecting SCI

Lesson Introduction

4. Objectives

As you know, there are several types of Sensitive Compartmented Information Facilities (SCIF) and mandated procedures for protecting SCI both inside and outside SCIFs as well as specific physical security measures to safeguard SCIFs. In this lesson, you will review the types of SCIFs and the requirements for properly protecting SCI material in your day-to-day work as well as what physical security measures are implemented to secure the SCIFs in which you work.

Here are the general lesson objectives:

- Identify the types of accredited SCIFs and their purposes
- Identify the proper methods for handling, discussing, reproducing, transporting, and destroying SCI material
- Identify the proper procedures for visitors and escorts in a SCIF

Here are additional lesson objectives for SSOs/SSRs:

- Identify the SCIF accreditation process
- Identify the components of the Fixed Facility Checklist

Sensitive Compartmented Information Facilities

Types of SCIFs

As you'll recall, there are three primary types of SCIFs: closed storage SCIF, open storage SCIF, and Continuous Operation SCIF. All three types of SCIFs are used to handle, process, discuss, and store SCI.

In closed storage SCIFs and Continuous Operation SCIFs, SCI must be stored in GSA-approved security containers. In open storage SCIFs, SCI may be stored in the SCIF, but GSA-approved security containers are not required. Because SCI may be stored in these types of SCIFs, they must be constructed in accordance with IC Tech Spec – for

ICD/ICS 705. Closed storage SCIFs require a 15 minute alarm response time while Open Storage and Continuous Operation SCIFs require a 5 minute alarm response time. Continuous Operation SCIFs are staffed and operated 24 hours per day 7 days per week.

SCIFs are primarily located in buildings, but can also be located in other areas.

g. Other SCIF Locations

SCIFs can be located aboard military surface and sub-surface vessels, or aboard military aircraft, or they can be Ground-based Temporary SCIFs (T-SCIFs), or Secure Working Area SCIFs. Details can be found in the Tech Spec.

Physical Security Measures: Inside SCIF

Review the physical security measures used inside a SCIF as well as those used to secure a SCIF.

a. Windows

Windows in a SCIF must be secured if they are at ground level or up to 18 feet above ground level. Ground level windows in a Closed Storage SCIF require security protection against forced entry, vision, sound attenuation, and compromising emanations.

b. Walls

Walls in SCIFs must extend from true floor to true ceiling and require acoustical protection measures and sound masking systems to protect SCI. Perimeter walls and internal compartment walls in a SCIF must meet specific sound attenuation standards (45 Sound Transmission Class, or STC). Large conference rooms that use Video Teleconferencing (VTC) must meet an even higher standard (50 STC). SCIFs in uncontrolled buildings require TEMPEST controls, which are technical countermeasures to contain compromising emanations inside the SCIF.

c. Intrusion Detection System (IDS)

SCIFs require an Intrusion Detection System (IDS) that will detect attempted or actual unauthorized human entry into a SCIF. SCIF Intrusion Detection Systems must meet the requirements of IC Tech Spec for ICD/ICS 705 and UL 2050. As outlined in UL 2050, one company must be responsible for the installation, maintenance, and monitoring of the IDS.

d. Telephone

A SCIF requires a telephone system that thwarts electronic eavesdropping on conversations inside the SCIF. Non-secure telephone systems must meet the Telephone Security Group (TSG) standard. Secure telephone systems must meet standards outlined in IC Tech Spec for ICD/ICS 705.

e. Fixed Facility Checklist (for SSO/SSR review)

The SCIF Fixed Facility Checklist (FFC) is located in IC Tech Spec for ICD/ICS 705 and is the checklist used to obtain accreditation for SCIFs. SSOs and SSRs must be familiar with the components of the FFC, which includes sections that cover general information about the SCIF; peripheral security, which means security for the building in which the SCIF is located; SCIF security; doors; details about the SCIF IDS; the SCIF's telecommunications systems and equipment; the SCIF's acoustical protection; the SCIF's classified destruction methods; and the information security, TEMPEST, and technical security information for the SCIF.

Physical Security Measures: Outside SCIF

Review the physical security measures used outside a SCIF that are used to secure access to the SCIF.

a. Doors

SCIFs require a solid entry door with a high security lock, such as a Kaba Mas CDX-07, CDX-08, or CDX-09 lock or a Sargent and Greenleaf, or S&G, 2890 PDL lock, and an access control system. SCIF emergency exit doors are the biggest vulnerability in forced entry and must be equipped with a deadbolt into a metal frame or strike plate and panic hardware with an audible alarm.

b. Access Control

For unattended SCIF entry, the access control system must use authentication and verification, such as an access card and personal identification number (PIN). For access to SCIFs during business hours, use cipher locks for high security areas and compartments. However, SCIFs should never be left unattended and protected only by access control.

How You Protect SCI

1. Getting Started

Try the Protecting SCI activity below. This activity will give you a chance to review the types of things that have implications for protecting SCI.

Here's how it works. You'll review access procedures for a SCIF at the visitor entrance to a SCIF. Next you'll review procedures for working in a SCIF as well as procedures for properly closing a SCIF. In addition, you will review the procedures you must follow to protect SCI outside of a SCIF.

The items in each setting might have consequences for how you handle and protect SCI. For each item, you'll be presented with useful information about that item or you will be asked a question about that item and will receive feedback to your answer.

2. Accessing the SCIF

Review the policies that relate to protecting SCI at the visitor's desk in a SCIF. Susan Jones and Ken Johnson are here to visit the SCIF today.

a. Visitor Control Log

Are Susan Jones and Ken Johnson required to record their citizenship on the visitor control log?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Visitor Control Log Feedback: Yes, Susan and Ken are required to record their citizenship. All visitors to SCIFs must record the following information on the visitor control log:

- Visitor's name and organization
- Visitor's citizenship
- Purpose of the visit
- Point of contact in the SCIF
- Date and time of visit

b. Visitor One

Susan Jones has not obtained a visitor certification. Should she be allowed to enter this SCIF?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Visitor One Feedback: Yes, Susan may enter the SCIF without a visitor certification as long as she is escorted by authorized DoD civilian or military personnel assigned to the SCIF. Escorts must also be indoctrinated with their escort responsibilities. However, since she is not certified, Susan will not be allowed access to classified information, regardless of her affiliation or position.

c. Visitor Two

Ken Johnson has a visitor certification. Does he require an escort to enter this SCIF?

- ○ Yes
- ○ No

Ken Johnson has a TOP SECRET/SCI clearance. What else must he have in order to enter certain areas of the SCIF?

- ○ High level position
- ○ Seniority
- ○ Need-to-know

See the next page for the correct answers and an explanation.

Visitor Two Feedback: Yes, Ken must be escorted. Escorts are required for all visitors. Only personnel who are assigned to a SCIF can enter without an escort.

Ken must also have need-to-know. Access to certain areas and to classified information is limited based on need-to-know required for official business.

d. Escort

Danielle Stilz works in this SCIF and she has come out to meet Ken and Susan. Can Danielle be an escort for either visitor in the SCIF?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Escort Feedback: Yes, Danielle can be their escort. All personnel assigned to the SCIF are authorized to escort non-indoctrinated or contractor personnel within the government area. However, prior to assuming escort duties, they must be briefed on their escort responsibilities.

Escort Responsibilities. Remember:

- Alert SCIF occupants verbally and/or with a warning light that an uncleared visitor is in the area.
- Walk with and observe uncleared personnel at all times until the visitor leaves or another escort assumes the duty.
- Ensure co-workers turn over, cover with an SCI cover sheet, or store classified material so that it cannot be seen by the visitor.

e. Visitor Certifications

As you know, each SCIF must have written procedures, established by the SCIF's SSO, for identifying and controlling visitors. Who processed Ken Johnson's visitor certification?

- ○ SCIF SSO or SSR
- ○ Person manning the SCIF visitor desk
- ○ Cognizant Security Authority (CSA)

See the next page for the correct answer and an explanation.

Visitor Certifications Feedback: The SSO or SSR process all SCIF visitor certifications.

f. Database for Personnel Access

Which is the primary database used for personnel access to SCIFs outside DoD?

- ○ Joint Personnel Adjudication System (JPAS)
- ○ Scattered Castles
- ○ Defense Special Security System (DSSS)

See the next page for the correct answer and an explanation.

Database for Personnel Access Feedback: Scattered Castles is used to the greatest extent possible by the CSA for access control to SCIFs. DoD information is furnished to Scattered Castles by DISS.

3. Inside the SCIF

Review the items that have implications for protecting SCI inside the SCIF.

a. Storage Containers

As you know, SCI must be stored within an accredited SCIF. Is SCI always required to be stored in a GSA-approved storage container?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Storage Containers Feedback: No, not always. SCI is not required to be stored in a GSA-approved storage container in an Open Storage SCIF, but is required to be stored in a GSA-approved container in a Closed Storage SCIF.

b. Transporting SCI

Tom Jameson has an SCI document he needs to share with Janie Calico, who works in another SCIF. What would be the preferred method for Tom to use to get the document to Janie?

- ○ Defense Courier Service (DCS)
- ○ Secure email or other secure electronic means
- ○ SCI-indoctrinated personnel

See the next page for the correct answer and an explanation.

Transporting SCI Feedback: If at all possible, Tom should send the document to Janie via secure email or secure electronic means. However, when it's not possible to transport SCI electronically, other authorized methods for transporting SCI may be used. These methods include hand-carrying by SCI-indoctrinated personnel in a manner that ensures proper protection, certified or designated couriers who possess a letter, memorandum, separate badge, or other written device such as DD Form 2501, Courier Authorization, attesting to their specific designation as an SCI Courier, diplomatic pouch, or the Defense Courier Service (DCS).

c. Packaging SCI

Remember: SCI material must be double wrapped prior to giving the package to the courier. SCI couriers must be appointed in writing and must have a signed original letter of authorization by the appropriate approving authority when travelling aboard U.S. commercial aircraft. SCI couriers must be familiar with all rules and regulations governing couriers and transporting classified information, including hand-carrying aboard military, U.S. Government chartered, or commercial aircraft. Specific instructions may be found in DoDM 5105.21, Volumes 1–3, Department of Defense Sensitive Compartmented Information Administrative Security Manual.

d. Bringing IS components and media into a SCIF

Tom Jameson brought a Government issued laptop from another agency into his SCIF this morning. Who was required to scan and approve the laptop?

- ○ CSA or ISSO
- ○ ISSO or SSO
- ○ SSR or SSO

See the next page for the correct answer and an explanation.

Bringing IS components and media into a SCIF Feedback: The SCIF's Information Systems Security Officer (ISSO) or the Special Security Officer (SSO) had to scan the laptop and approve it before he was allowed to bring it into the SCIF. No IS components, media, and/or memory may be brought into a SCIF or removed from a SCIF unless it has been properly logged and approved by the ISSO or SSO.

e. Connecting classified and unclassified systems together

Without consulting anyone, Tom Jameson decided to connect two computers together in his office so he could transfer files between the two. One computer was classified and the other was unclassified. Was it OK for Tom to connect these two computers together?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Connecting classified and unclassified systems together Feedback: No, Tom should not have done that because it is prohibited to connect classified and unclassified systems together. Additionally, you must never transfer information that resides on a classified system onto an unclassified system without proper authorization.

f. Borrowing passwords

Danielle cannot remember the new password she created for her access to the unclassified system in her SCIF. She is in a hurry, so she just asked Tom to borrow his password temporarily. Should Tom allow Danielle to borrow his password?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Borrowing Passwords Feedback: No, Tom should not allow Danielle to borrow his password. You must never share or compromise your passwords no matter what classification the system is. Also, remember you must create smart passwords following your organization's guidance and memorize them rather than write them down.

4. Copy Area in a SCIF

Review the items that have implications for protecting SCI inside the copy area in a SCIF.

a. SCI Destruction Guidelines

Remember: Destruction of SCI must occur on a daily basis by SCI indoctrinated personnel and must be accomplished in a manner that precludes intelligible reconstruction. Also, having an emergency destruction plan is a good best practice and may even be required by circumstances or by your customer.

b. SCI Destruction Methods

Is shredding the only way to destroy SCI material?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

SCI Destruction Methods Feedback: No, there are other methods for destroying SCI. Other Director of National Intelligence (DNI) approved methods for destroying SCI include burning, pulping, pulverizing, melting, and chemical decomposition. Note that residue from destroyed SCI must not be left in clear plastic bags for uncleared personnel to see.

As you may recall, crosscut shredders, pulpers, and other destruction equipment used to destroy SCI paper materials must be on the NSA Evaluated Products List of High Security Crosscut Paper Shredders, and must be the same type used for the terminal destruction of COMSEC paper products. Note that SCI in computer or automated systems or other magnetic media must be destroyed by sanitizing using approved degaussing equipment and then pulverized using an approved disintegrator.

c. Reproduction of SCI

Remember:

- Reproduction equipment must display the highest level of classification allowed to be reproduced on that equipment.
- Copiers may not be used for reproducing SCI if they leave latent images on themselves or other material or if they connect to remote diagnostic centers, such as by telephone line.
- Copies of classified documents are subject to the same control, accountability, and destruction procedures as the original document.

5. Closing the SCIF

Kelly Turner is about to close her SCIF for the day. Review the items that have implications for properly closing a SCIF.

a. Before setting the alarm

Before Kelly sets the alarm, she must verify that all computer systems are logged off and that she is the last one there. Kelly's SCIF is a closed storage SCIF, so she must ensure that no classified material is left out. Kelly must also verify that all security containers are closed and locked and that the closed sign is displayed on each security container and the SF-701 form has been completed.

b. After setting the alarm

After Kelly sets the alarm and leaves the SCIF, she must spin the lock on the door, display the closed sign, and complete the SF-702 form.

6. Outside the SCIF

Tom and Tracy Jameson are married, and both are civilians who both work for a major defense contractor. Tom works in a SCIF. Tom and Tracy are arriving home from work and stop to speak to their neighbor, Eric Goodfellow, who is a military officer. Review the items that can have implications for protecting SCI outside of your SCIF.

a. Identification

Who should not be wearing their name badge?

- ○ Tom Jameson
- ○ Tracy Jameson
- ○ Eric Goodfellow

See the next page for the correct answer and an explanation.

Identification Feedback: Tom Jameson should not be wearing his name badge because he is outside of his SCIF. When outside of your SCIF, you must not call attention to yourself. You must remove your name badge as soon as you leave your SCIF.

b. Talking about your work with family

Who must Tom consult to find out what he can tell Tracy about his work location and mission?

- ○ ISSO
- ○ SSO
- ○ SSR

See the next page for the correct answer and an explanation.

Talking about your work with family Feedback: Tom must consult his SCIF's Special Security Officer (SSO) to learn what he is and is not permitted to tell his wife, Tracy, about his location and mission.

c. Talking about your work with other cleared personnel

Since Eric is a neighbor and he is a military officer, is it OK for Tom to talk about his work with Eric?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Talking about your work with other cleared personnel Feedback: No, Tom should not discuss his work with Eric. As you know, you must not discuss SCI outside of your SCIF with anyone.

Remember: Being aware of your surroundings both inside and outside the SCIF and knowing the policies and procedures you need to apply will help you and your organization properly protect SCI.

Student Guide

Course: Sensitive Compartmented Information (SCI) Refresher

Lesson 5: SCI Reporting Requirements

Lesson Introduction

5. Objectives

As you know, you have access to SCI because the United States Government has put its trust in you. This relationship obligates you to report certain events and incidents to your security office, which range from specific information about your personal life to security incidents that have caused the loss or compromise of classified information. In this lesson, you will review the types of information that you, as an individual with access to SCI, are required to report.

This is the lesson objective:

- Recognize the types of information that must be reported by or about individuals who have SCI access

Knowing What to Report

1. Getting Started

Try the SCI Reporting Requirements activity. This activity will give you a chance to review the kinds of things that must be reported by or about those who have access to SCI. Here's how it works. You'll read the stories of employees who have access to SCI, which obligates them to certain reporting requirements, and you will be asked to determine whether the information you learned about that person is required to be reported or not. For each question, you'll be presented with feedback to your answer.

2. Conference Room

a. Shannon O'Connor

Shannon O'Connor recently got married but she did not take her new husband's last name. Is Shannon required to report her marriage?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Shannon is required to report her marriage whether she changes her last name or not. In fact, everyone who has access to SCI is required to report any changes in personal status such as marriage, separation, divorce, and cohabitation.

b. Mark Conley

Mark Conley has been visiting the casinos on a regular basis and has incurred over $100,000 in debt due to gambling. Is Mark required to report his gambling problem?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Mark is required to report his gambling problem. Everyone with SCI access must report personal problems such as drug and alcohol misuse or abuse and financial problems.

c. Gene Sanders

On Friday evening, Gene Sanders went out drinking with his buddies. On his way home, he was arrested for DUI. This is the first time this has ever happened to him. Is Gene required to report his arrest?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Gene is required to report his arrest for DUI. In fact, personnel with SCI access are required to report *all* legal involvements such as litigation, arrests, and court summons.

d. Robin Queen

Robin Queen knows that Jack Bell, her co-worker and friend, has not been paying child support and has to attend a court hearing next week. Jack says this is a personal issue and that it is not his employer's business, even though he has SCI access. Should Robin report the fact that Jack has been summoned to court for not paying child support since she knows that he won't report it?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes. Although Jack should be the one to report this information, Robin is obligated to report it since she knows that Jack will not. Everyone with SCI access is required to report adverse information about others who also have SCI access.

e. Jason Wu

A reporter from the local newspaper contacted Jason Wu about the controlled access program, Bluebell. Jason told the reporter he's never heard of Bluebell and did not provide any other information. Since Jason didn't share any information about Bluebell with the reporter, is he required to report this phone contact?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Jason is required to report this contact with the reporter. All personnel with access to SCI are required to report any contact with the media. In addition, they are required to report any improper solicitations for information. Note that this call from the local newspaper reporter could also be considered an improper solicitation for information because the information is classified.

f. Helen Brown

Helen Brown enjoys meeting her girlfriends for drinks and appetizers most Friday evenings before attending a movie with them. Is Helen required to report her alcohol consumption?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: No, Helen is not required to report her occasional and moderate alcohol consumption. Personnel with access to SCI are required to report their alcohol consumption, or the alcohol consumption of their co-workers who have SCI access, only if that alcohol consumption is a problem.

3. Office Area in the SCIF

a. Paul Coble

Paul Coble left an SCI document in a folder in his desk drawer when he left work yesterday. He forgot to put it back in its security container before he left work. After discussing this incident with his supervisor, they determined the information was most likely not compromised. Does this incident require reporting?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, this incident must be reported. When rules have not been followed, resulting in a possible compromise of classified information, a report must be made. These types of security incidents are called infractions.

b. Janice Bowers

Janice Bowers has recently noticed that one of her co-workers in the SCIF has become disgruntled and very unhappy. Should Janice report her co-worker's disgruntled behavior?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Janice must report her co-worker's behavior. All personnel with access to SCI must report disgruntled employees in the SCIF.

c. Kevin Connolly

Kevin Connolly works for a defense contractor and has been asked to give a presentation at a symposium next month regarding his area of expertise, which is of a classified nature. Is Kevin required to have his presentation reviewed prior to the symposium?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Kevin must have a pre-publication review of his material. All personnel with access to SCI are required to have a pre-publication review of any material they create before it enters the public domain. This includes works of fiction, speeches, articles, white papers, advertisements, web pages, web sites, blogs, chat rooms, and video teleconferences.

4. Copy Area in the SCIF

a. Bob Moore

Today when Bob Moore started to leave his building for lunch, he overheard his co-worker in the stairwell discussing on a cell phone the controlled access program they have been working on together. Should Bob report his co-worker?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Bob must report this incident since the co-worker's conversation is an unauthorized disclosure. It does not matter who the co-worker was talking to. SCI is not to be discussed outside of the SCIF to anyone. All personnel who have access to SCI must report unauthorized disclosures to their immediate supervisor and their security office only. Unauthorized disclosures include leaks, which are deliberate disclosures of classified information to the media, and spills, which are accidental or intentional disclosures of classified information across computer systems.

b. Rosa Gonzalez

This morning, Rosa Gonzalez noticed that Mr. Johnson arrived at the SCIF an hour earlier than usual today. Should Rosa report this information about Mr. Johnson?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: No, Rosa should not report Mr. Johnson for arriving to work an hour early. It's possible that Mr. Johnson just came in early to work on something for which he has an urgent deadline. Or perhaps he must leave the SCIF early today for a doctor's appointment. However, if this type of behavior continues without an explanation, then it might make sense for Rosa to report it. In general, though, suspicious co-worker activities must be reported by all personnel with access to SCI.

c. Richard Phillips

Richard Phillips is making copies of SCI documents with the intention of putting them in his briefcase so he can work on them at home. If anyone sees Richard remove these copies of SCI documents from the SCIF, are they required to report it?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, this must be reported. It is a security violation because it involves the loss, compromise, or suspected compromise of classified information. All personnel with SCI access must report security violations.

d. Sandy Tully

Sandy Tully recently joined an anti-military activist group called No War for US. Is Sandy required to report her affiliation with this group?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Sandy is required to report her affiliation with this group. You must report any external activist groups that you or anyone you work with belong to.

5. Foreign Interactions

a. Howard Brewer

Not only is Howard Brewer a well-respected employee, but he is also a great husband because he is taking his wife to Hawaii to celebrate their 30th anniversary. Was Howard required to report that he was taking this trip?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: No, Howard is not required to report his trip to Hawaii because it is within the U.S. However, Howard Brewer and all personnel who have SCI access are required to report all foreign travel prior to departure. The only exception to this rule is that day trips to Canada and Mexico may be reported upon return. In addition, all unusual incidents on any trip must be reported and some foreign trips may require a pre-travel briefing.

b. Trish Rivers

Trish Rivers recently she began dating a French businessman who lives near her. This man has French citizenship and is not a U.S. citizen. Is Trish required to report this relationship?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Trish is required to report that she is dating this man from France because he is a French citizen and not a U.S. citizen. All personnel who have SCI access are required to report close continuing relationships, whether they are personal or business, with a citizen, resident, or representative of a foreign country. This rule also includes foreign contacts via the Internet such as email and chat rooms.

c. Chris Cohen

Chris Cohen travelled to Canada on a business trip for his job with a defense contractor. While he was in Canada, Chris attended a gala at the U.S. Embassy in Canada and mingled with several Canadian citizens. Is Chris required to report these foreign contacts?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: No, Chris does *not* have to report these *casual* foreign contacts from the gala. Chris Cohen and all personnel who have access to SCI are only required to report casual foreign contacts if the foreign contact displays a strong interest in the person's employment, is not satisfied with answers provided to their questions, or if the foreign contact requests or attempts to have follow up contact.

d. Lillian Cho

Lillian Cho works for a defense contractor full-time but recently took a part-time position working on the weekends for a furniture store that is a Swiss-based company. Is Lillian required to report her part-time employment?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, Lillian is required to report her part-time job because it is for a foreign-based company. All personnel with SCI access must report any foreign-based outside employment.

e. Shawna Smith

Shawna Smith is travelling to deliver an SCI document to another SCIF. However, she switched bags before she left and forgot to put her courier card in the bag she was carrying on her trip. It was an honest mistake. When Shawna arrives at her destination without her courier card, should the person to whom she is delivering the document report the fact that Shawna did not have her courier card even though Shawna has the appropriate clearance eligibility and need-to-know?

- ○ Yes
- ○ No

See the next page for the correct answer and an explanation.

Feedback: Yes, the fact that Shawna forgot to bring her courier card must be reported. You must report any systemic weaknesses and anomalies.

Conclusion

1. Lesson Objectives

Congratulations! You have completed the SCI Reporting Requirements lesson. It is essential that you understand what you are required to report about yourself and others in order to protect SCI and our nation's security.

Student Guide

Course: Sensitive Compartmented Information (SCI) Refresher

Lesson 6: Course Conclusion

Course Summary

In this course, you reviewed your obligations to protect SCI as outlined in the SCI Nondisclosure Statement you signed. You also reviewed the ways you must protect SCI both inside your SCIF and outside your SCIF.

Lesson Review

Here is a list of the lessons in the course:

- Course Introduction
- SCI Fundamentals
- SCI Control Systems and Markings
- Protecting SCI
- SCI Reporting Requirements
- Course Conclusion

Course Objectives

You should be able to:

- ✓ Recognize SCI policy guidance documents
- ✓ Identify the purpose and components of the Sensitive Compartmented Information (SCI) Nondisclosure Statement (NdS)
- ✓ Apply classification markings and dissemination controls for SCI materials
- ✓ Identify the proper methods for handling, discussing, reproducing, transporting, and destroying SCI material
- ✓ Identify the proper procedures for visitors and escorts in a SCIF
- ✓ List the types of accredited SCIFs and their purposes
- ✓ Recognize the types of information that must be reported by or about individuals who have SCI access

In addition, the SSO/SSR should be able to:

- ✓ Identify the process for SCI indoctrination and pre-screening
- ✓ Identify the SCIF accreditation process
- ✓ Identify the components of the Fixed Facility Checklist

Conclusion

Congratulations. You have completed the *Sensitive Compartmented Information Refresher* course. Throughout this course you have had an opportunity to practice applying all of the listed activities.

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