Temporary Sensitive Compartmented Information Facility (T-SCIF)

Student Guide

February 19, 2023

Center for Development of Security Excellence

TABLE OF CONTENTS

T-SCIF COURSE INTRODUCTION

INTRODUCTION

Welcome to the Temporary Sensitive Compartmented Information Facility, or T-SCIF, course. All personnel with access to classified information must maintain a heightened sense of awareness and immediately take action to report all instances of suspicious and malicious behavior to their Security Office, Special Security Office, Contractor Security Office, and/or Chain of Command.

This course is intended to:

- Provide guidance for the approval and operation of T-SCIFs, when required, in support of tactical, contingency, emergency, and other immediate operational needs
- Ensure the execution and protection of a sound command security program to protect classified information and prevent unauthorized disclosure

There are knowledge checks throughout the course, and these are not scored. However, at the end of the course is a cumulative assessment. You must pass this final test with at least a score of 80% to qualify for a Certificate of Completion.

COURSE OBJECTIVES

By the end of this course you should be able to:

- Define Sensitive Compartmented Information, or SCI, and T-SCIF
- Recognize National Security Policy and SCI Authorities
- Identify SCI Leadership Responsibilities
- Identify Required Documentation for T-SCIF
- Explain T-SCIF Security Requirements
- Describe Examples of T-SCIF Configurations
- Discuss how SCI is Stored and Destroyed
- Create a T-SCIF Emergency Action Plan (EAP)
- Properly Report Security Incidents & Violations

LESSON 1: WHAT IS A SCI, A T-SCIF, AND WHO CONTROLS THE PROGRAM?

INTRODUCTION

What is SCI, T-SCIF, and Who Controls the Program? Let's start by talking about some of the types of information we are concerned about.

WHAT IS SCI

SCI is classified national intelligence concerning, or derived from, intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence. Access to SCI is closely controlled and granted only after a clear need-to-know for such access has been established.

CUI

Controlled Unclassified Information, or CUI, is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. The loss or improper safeguarding of CUI could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

Now we will talk about classified information which is divided into one of three categories.

CONFIDENTIAL

Confidential applies to information or material the unauthorized disclosure of could reasonably be expected to cause damage to the National Security.

SECRET

Secret applies to information or material the unauthorized disclosure of could reasonably be expected to cause serious damage to the National Security.

TOP SECRET

Top Secret applies to information or material the unauthorized disclosure of could reasonably be expected to cause exceptionally grave damage to the National Security.

IN ADDITION

In addition to the above, some classified information is so sensitive that even the extra protection measures applied to Top Secret information are not sufficient. This information is known as "Sensitive Compartmented Information" (SCI).

WHAT IS A T-SCIF

T-SCIF Definition. Temporary SCIFs (T-SCIFs) are used by Combatant Commands (CCMDS) and Military Departments (MILDEPS) in support of tactical, contingency, and field-training operations for a limited time where physical security construction standards associated with permanent facilities are not possible.

T-SCIFs are spaces approved for the use, handling, and storage of SCI material. They may include hardened structures (buildings, bunkers, etc.), truck-mounted or towed shelters, tents, prefabricated modular trailers or buildings, and areas used on aircraft and surface/sub-surface vessels.

These facilities are designed to be temporary and not to exceed one year without mission justification and approved by the Accrediting Official (AO).

Permanent-type hardened structures shall be used to the greatest extent possible for T-SCIFs.

Prior to the T-SCIF activation, the Accrediting Official (AO) may require submission of a Fixed Facility Checklist (FFC), whether it be for a ground-based operation, a FFC Aircraft Checklist, a Shipboard/Submarine FFC, or a T-SCIF Checklist produced before or after a deployment.

WHO OWNS THE PROGRAM?

E.O. 13470 amended E.O. 12333 and established the Director of National Intelligence (DNI) as the Head of the Intelligence Community for intelligence matters related to national security. DNI oversees and directs the implementation of the National Intelligence Program.

LESSON 1: KNOWLEDGE CHECK

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson One: What is SCI, Temporary SCIF, and Who Controls the Program? Now, let's test your comprehension of the material with a knowledge check. Please select Next to begin.

KNOWLEDGE CHECK 1

SCI is classified national intelligence concerning, or derived from, intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

Select True or False. Then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

LESSON 2: NATIONAL SECURITY POLICY AND SCI AUTHORITIES

INTRODUCTION

This lesson will cover the policies and authorities that have been put in place to assure the security of sensitive compartmented information.
Select 'Next' to continue.

NATIONAL SECURITY POLICY

To start, select each cell in the table below to see a short explanation of what each of these Executive Orders, DOD Regulations and Manuals, and Intelligence Community, or IC, Directives contain.

- Executive Order 12333 as amended by EOs 13284, 13355, and 13470
  Executive Order (EO) 12333, "United States Intelligence Activities", as amended by EO 12384, 13355, and 13470 is the authority for U.S. Intelligence Activities.
  - Established the Senior Officials of the Intelligence Community (SOICs) as the authority within their military departments or agencies to protect intelligence and intelligence sources and methods from unauthorized disclosure consistent with guidance from the Director of Central Intelligence.
  - Designates the Director of National Intelligence (DNI) as the head of the Intelligence Community (IC) for intelligence matters related to national security. The DNI shall oversee and direct the implementation of the National Intelligence Program

- Executive Order 13526. Classified National Security Information
  - Prescribes a uniform system for classifying, safeguarding, and declassifying National Security Information (NSI) including information relating to defense against transnational terrorism

- DODM 5105.21, Volume 2 "Sensitive Compartmented Information (SCI) Administrative Security Manual is the SCI Administrative Security Manual

- Identifies DIA/DAC as the sole accrediting authority for DOD SCI Facilities
- Prescribes security policy and procedures for the protection, use, and dissemination of SCI within DOD SCI Facilities

- Department of Defense Instruction DODI 5200.01 "DOD Information Security Program and Protection of Sensitive Compartmented Information (SCI)"
  - Updates policy and assigns responsibilities to Defense Intelligence Agency (DIA) to inspect and accredit DOD SCI Facilities for handling, processing, storage and discussion of SCI

- Intelligence Community Directive (ICD) 705, "Sensitive Compartmented Information Facilities"
  - Establishes that all IC SCIFs shall comply with the uniform IC physical and technical security requirements
  - Designed to ensure the protection of SCI and foster efficient, consistent, and reciprocal use of SCIFs in the IC
  - Applies to all facilities accredited by IC elements where SCI is processed, stored, used, or discussed

- Intelligence Community Standard (ICS) 705-1, "Physical and Technical Security Standards for Sensitive Compartmented Information Facilities"
  - Sets forth the physical and technical security standards that apply to all SCIFs, 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
  - 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
  - States that the Assistant Deputy Director of the National Intelligence for Security shall, in consultation with IC elements, develop and establish technical specifications to implement SCIF standards that include descriptions of best practices

- Intelligence Community Standard (ICS) 705-2, "Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Facilities"
  - Sets forth the criteria that apply to the accreditation of SCIFs 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, "Intelligence Community Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities" contains the physical and technical security specifications and best practices
  - Sets forth the physical and technical security specifications and best practices for

meeting standards of ICS705
- Is the implementing specification for ICD 705 and ICS 702-1
- Facilitates the protection of SCI against compromising emanations, inadvertent observation and disclosure by unauthorized persons, and the detection of unauthorized entry
- CNSSAM TEMPEST Red/Black Separation is discussed within this IC Tech Spec

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

For more information on DOD Directives and DNI Counterintelligence & Security Governance/Regulations, please use the links located on the resources page.

You have completed Lesson Two, National Security Policy and SCI Authorities. Now participate in a knowledge check to test your comprehension of the material.

Select 'Next' to begin the knowledge check.

KNOWLEDGE CHECK 1

What identifies DIA Counterintelligence and Security Office (DAC), as the sole accrediting authority for DOD SCI Facilities?
Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐ICD 700
☐DODM 5105.21, Vol. 2
☐EO 12333, as amended

KNOWLEDGE CHECK 2

Which of the following establishes control over SCI?
Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐EO 13470
☐EO 12333, as amended
☐DODM 5105.21, Vol.2
☐ICD 700
☐DODI 5200.01

LESSON 3: SCI LEADERSHIP RESPONSIBILITIES

INTRODUCTION

SCI Leadership Responsibilities describes the SCI Community network and provides a listing of leadership responsibilities. It also includes the training requirements for those involved with SCI.

SCI COMMUNITY NETWORK

The SCI Community Network is composed of all personnel assigned the responsibility of managing, safeguarding, storing, and/or transmitting intelligence information over a SCI Network.

This includes but is not limited to: Special Security Officers (SSOs), Special Security Representatives (SSRs), and Information Assurance Managers (IAMs) in your chain of command, your SCI Program Managers, and SSO Defense Intelligence Agency (DIA). All of these resources are available to support you!

NOTE: All branches of the military have the same organization structure under their respective Head of Intelligence Community Element (HICE). Also, when deployed, SSOs will follow Combatant Command (COCOM) representative guidelines.

Select the information icons to receive more information. You must select all of the icons before you can proceed.

SCI LEADERSHIP RESPONSIBILITIES

Director of DIA

- Administers uniform DOD SCI policy for:
  - Physical security
  - Technical security (TEMPEST and technical surveillance countermeasures or TSCM)
  - Information security
  - Personnel security
  - Automated Data Processing (ADP, ADP-II, & ADP-III) security
  - Security education and awareness
  - Contractor SCI program administration to implement and supplement National Board, or NIB and DNI SCI policy
- Administers DNI security policy and procedures consistent with DNI policies and procedures to protect intelligence and intelligence sources and methods within DOD.

- Accredits, inspects, approves waivers, and de-accredits DOD SCIFs to ensure compliance with DNI/DOD policy.
- Develops and coordinates recommendations regarding DNI security policy.

HICE

The Head of Intelligence Community Element, or HICE, of each military service administers the SCI security program for their respective Departments and component command of the Combatant Commands. Provides implementing instructions for the operation and administration of SCI security programs for their respective agencies, departments, and components, including subordinate commands of the Combatant Commands.

Heads of DOD Components that are not Elements of the Intelligence Community, shall appoint, at an appropriate level, a senior intelligence officer, or SIO who shall be responsible for the overall management of SCI programs. The appointment shall be reported to DIA and the Under Secretary of Defense for Intelligence and Security, or USD (I&S).

Cognizant Security Authority (CSA)

The CSAs shall, as delegated by the HICE, have authority over and responsibility for all aspects of management and oversight of the security program established for the protection of intelligence sources and methods, and for implementation of SCI security policy and procedures defined in DNI policies for the activities under their purview. CSAs may formally delegate this responsibility to specific elements within their organization.

Senior Intelligence Officer (SIO) Responsibilities

Responsible for the command's SCI security program. Provide proper protection, use, and dissemination of SCI documents and material by enforcing SCI, information, personnel, physical, communication, industrial, and IA security rules and by developing standard operating procedures, or SOPs, and practices. Exercises overall management of SCI programs.

Special Security Officer (SSO) Responsibilities

Manage the SCI security program and oversee SCI security functions for subordinate SCIFs. Supervise the operation of the special security office and administer the SCI security program to include SCI security oversight for other SCIFs and T-SCIFs under the organization's security cognizance. Properly account for, control, transmit, package, and safeguard SCI. Maintain appropriate accreditation documentation for each SCIF, communications system, and Information System, or IS under the organization's cognizance.

Special Security Representative (SSR) Responsibilities

The SSR, under the direction of the SSO, is responsible for the day-to-day management and implementation of the facility's SCI security program for subordinate SCIFs and T-SCIFs. SSRs perform one or more of the SSO duties as delegated and agreed to by their SSOs.

REQUIRED TRAINING

The major organizations providing SSO training are the DIA, and Office of the Director of National Intelligence (ODNI), including the SCI Security Officials Course (SSOC).
All personnel assigned to the position of SSO will attend the SCI Security Officials course within 120 days of being appointed to these security duties. SSOs will train SSRs within 30 days of their assignments to the SSR position and:

- Provide annual refresher training and maintain strategic communications with SSRs and security managers
- Provide security training to subordinate commands for T-SCIF operations and further safeguarding of classified information during the redeployment phase
- When possible SSRs are allowed attendance at the Security Officials course as a security Baseline
- SSRs will still receive annual refresher training from SSOs

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Three, SCI Leadership Responsibilities. The following knowledge check will assess your command of the lesson's material. Please, select 'Next' to begin.

KNOWLEDGE CHECK 1

All personnel assigned to the position of SSO will attend the SCI Security Officials course within how many days of being appointed?

Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐30 days
☐60 days
☐120 days

KNOWLEDGE CHECK 2

Who administers uniform DOD SCI policy for Physical Security and Information Security?
Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐Director of DIA
☐Head of Intelligence Community Element
☐Cognizant Security Authority

LESSON 4: T-SCIF OVERVIEW

INTRODUCTION

The T-SCIF Overview covers Planning Considerations, how to make a T-SCIF Request, and reviews certain required Policies, Procedures, and Standard Operating Procedures (SOPs).

PLANNING CONSIDERATIONS

Establishing a T-SCIF requires detailed planning and coordination. Here are procedures to follow:

- Provide proper protection, use, and dissemination of SCI documents and material by enforcing SCI, information, personnel, physical, communications, industrial, and Information Assurance security rules and by developing standard operating procedures also known as SOPs and practices in accordance with regulatory guidance
- Ensure SCI is disseminated to persons with authorized access to the material. They also must have an established "need-to-know"
- Ensure an Accrediting Official-approved Emergency Action Plan or EAP is developed and rehearsed periodically by all personnel assigned to the T-SCIF; the results of the rehearsal drills shall be documented
- Ensure SCI cleared personnel receive proper security education, training, and awareness and are trained to perform their respective duties and responsibilities in the protection of SCI and equipment
- Ensure when employing a T-SCIF, a risk management approach is used that balances the operational mission with the protection of SCI

T-SCIF PRE-DEPLOYMENT CONSIDERATIONS

SCIF security, temporary or permanent, starts with the decision to build a SCIF. Adequate planning and design will prevent many of the security risks to SCI. If you have been assigned responsibility for creating a T-SCIF, then site planning should have already taken place, including looking at the standoff distance for **Anti-Terrorist/Force Protection** (AT/FP) as well as TEMPEST requirements.

Pre-deployment considerations are covered in the T-SCIF Request which must be submitted at least 14 days prior to T-SCIF activation.

Other items to consider include:

- Access Control Procedures
- Visitor and Escorting Procedures

Let's start with the T-SCIF request.

T-SCIF REQUEST – REQUIRED INFORMATION

Information, timeframe, and format of submission may vary based upon Accrediting Official. IC Tech Specs for ICD/ICS 705 provides the baseline guidelines and forms for ground, surface/sub-surface vessels, and aircrafts. The Accrediting Official may require a variation of the form(s) to be completed and submitted as part of the approval process. You may select each of the IC directives to review.

ICD 705: Sensitive Compartmented Information Facilities

- Establishes that all IC SCIFs shall comply with the uniform IC physical and technical security requirement
- Designed to ensure the protection of SCI and foster efficient, consistent, and reciprocal use of SCIFs in the IC
- Applies to all facilities accredited by IC elements where SCI is processed, stored, used, or discussed
- Rescinds DCID 6/9, ICPM 2005-700-1, ICPM 2006-700-7, and ICPM 2007-700-2

ICS 705-1: Physical and Technical Security Standards for Sensitive Compartmented Information Facilities

- Sets forth the physical and technical security standards that apply to all SCIFs, 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
  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
- States that the Assistant Deputy Director of the National Intelligence for Security shall, in consultation with IC elements, develop and establish technical specifications to implement SCIF standards that include descriptions of best practices

ICS 705-2: Standards for the Accreditation and Reciprocal Use of Sensitive Compartmented Facilities

- Sets forth the criteria that apply to the accreditation of SCIFs 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: Intelligence Community Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.1 contains the physical and technical security specifications and best practices

- Sets forth the physical and technical security specifications and best practices for meeting

standards of ICS705

- Is the implementing specification for ICD 705 and ICS 702-1 and supersedes DCID 6/9
- Facilitates the protection of SCI against compromising emanations, inadvertent observation and disclosure by unauthorized persons, and the detection of unauthorized entry
- CNSSAM TEMPEST Red/Black Separation is discussed within this IC Tech Spec

REQUIRED INFORMATION FOR ARMY T-SCIF

It must be submitted at least 14 days prior to T-SCIF activation.

- Indicate parent SCIF ID# and Exercise/Operation Name, parent group SSO, and the name of your SSO
- Indicate where training will take place if it will be held at a different installation or command
- Indicate where you will be deployed from and the 8 digit map coordinates (if possible) of the deployment location
- Describe the facility to be used, and the type of T-SCIF configuration. For example, tents, shelters, vehicles, existing shelters, caves, etc.
- Provide dates of operation for STARTEX to ENDEX

Note that T-SCIFs will be 24-hour mode of operation. This cannot be waivered.

- Describe the physical aspects of the T-SCIF's defensive perimeter, and use of concertina
- Include the number, type and placement of guards fixed or roving, clearance level of guards, and access point. Provide nomenclature of guard's weapons and storage point of ammunition if applicable
- What are the type and classification level of SCI being processed or utilized. What is the nomenclature of systems used to process SCI?
- Will hardcopy SCI storage be required; if so, what is the nomenclature of the approved GSA security container?
- Is there proper sound attenuation for open discussion of SCI in the T-SCIF? If not, what countermeasures will be used? For example, power generator, white noise generators, etc.
- How many SSO/SSR personnel will be present per shift? There must be at least one SCI-cleared individual present at all times
- List the name, rank, unit, and contact number, if available for the SSO/SSR responsible for onsite operations of the T-SCIF
- Describe how the SCI will be stored
- Explain how SCI will be transported from the SCIF to the field site. Include means of

transportation, including couriers, and storage of SCI while in transit

Note: Couriers must be appointed on orders.

REQUIRED INFORMATION FOR AIR FORCE T-SCIF

Required Information for an Air Force T-SCIF includes:

Appointment Letters for
- Physical security
- Personnel security
- Information security

Accreditation letters for
- Physical security
- TEMPEST (should be accomplished/updated during aircraft Depot)
- Automated Information System (AIS)
- Video Teleconference (VTC)

Also required are:
- Fixed Facility Checklist (FFC)
- TEMPEST Addendum to FFC
- Security posture change, waivers, and exceptions to policy(s)
- DOD Threat Assessment
- Standard Operating Procedures
- Emergency Action Plan Aircraft Checklist

REQUIRED INFORMATION FOR NAVY T-SCIF

Required Information for a Navy T-SCIF includes:

Appointment letters for:
- Special Security Officer (SSO)
- Special Security Representative (SSR)
- Information Assurance Manager (IAM) Primary and Alternate

Accreditation Messages for
- T-SCIF MSG is also TEMPEST accreditation
- Automated Information System (AIS)

Also required are:
- Shipboard/Submarine Fixed Facility Checklist (FFC)

- Shipboard/Submarine T-SCIF Checklist
- DOD Threat Assessment
- SOP/Submarine INSTRUCTIONS FOR TSCIF OPERATIONS
- EAP/Submarine INSTRUCTIONS FOR EAP

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Four, T-SCIF Overview. Let's see how well you comprehend the material with a knowledge check. Select 'Next' to begin.

KNOWLEDGE CHECK 1

The Army T-SCIF Request must be submitted at least how many days prior to T-SCIF activities? Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐7 days
☐14 days
☐21 days

KNOWLEDGE CHECK 2

Appointment letters are required for both Air Force and Navy T-SCIFs.
Select True or False. Then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

LESSON 5: T-SCIF SECURITY REQUIREMENTS

INTRODUCTION

This lesson will discuss T-SCIF security requirements.

ARMY T-SCIF SECURITY REQUIREMENTS

Army T-SCIF Security Requirements:

- T-SCIF security features shall provide acoustical, visual, and surreptitious entry protection.
- A TSCM inspection shall be requested for any structure proposed for T-SCIF use if the space was previously occupied by a non-U.S. element. It is the AO's responsibility to evaluate operating the SCIF prior to TSCM inspection and formally assume all risk associated with early operation.

- When possible, T-SCIFs shall be established within the perimeters of U.S.-controlled areas or compounds.
- If a U.S.-controlled area or compound is not available, the T-SCIF shall be located within an area that affords the greatest degree of protection against surreptitious or forced entry.
- When a T-SCIF is in operation, the perimeter of its immediate area shall be observed and protected by U.S. guards with U.S. SECRET clearances. Guards shall be equipped with emergency communication devices and, if necessary, with weapons.
- During non-operational hours, the T-SCIF shall be provided security protection in accordance with AO guidelines.
- The T-SCIF shall have only one entrance which shall be controlled during hours of operation by an SCI-indoctrinated person using an access roster.
- Unclassified telecommunications equipment shall meet the requirements outlined in Chapter 10 of IC Tech Spec – for ICD/ICS 705 to the greatest extent practical.
- Telephones obtained in a foreign country shall not be used within a T-SCIF.
- Cables and wires penetrating the T-SCIF perimeter shall be protected. The AO may require inspections and routing of cables and wiring through protective distribution systems or may require other countermeasures.
- AO-approved emergency destruction and evacuation plans shall be developed and rehearsed periodically by all personnel assigned to the T-SCIF; the results of the rehearsal drills shall be documented.
- When in transit, ground-based and mobile (e.g., truck-mounted, towed military shelters) T-SCIFs containing unsecured and non-encrypted SCI shall be accompanied by a U.S. TOP SECRET-cleared individual with SCI access approval(s).
- During movement, T-SCIF structures shall be secured with GSA-approved locking devices and equipped with tamper-evident seals.
- When in transit, hardened T-SCIFs having no open storage of SCI may be monitored by a U.S SECRET-cleared individual.
- Hardened T-SCIFs shall be designed with TEMPEST countermeasures as identified by the CTTA; The AO, in collaboration with the CTTA, shall provide red/black separation and "protected distribution" guidance for field installation in accordance with CNSSAM TEMPEST 1/13 and CNSSI 7003.
- When a T-SCIF is no longer required, the responsible SCI security official shall conduct a thorough facility inspection to ensure all SCI material has been removed.

AIR FORCE T-SCIF SECURITY REQUIREMENTS

General Requirements for an Air Force T-SCIF

- A Secure Working Area (SWA) on an aircraft is an area accredited for the temporary use, handling, discussion and/or processing of SCI but where SCI is not normally stored, i.e., approved, dedicated military aircraft w/classified SCI onboard.
- The SWA is defined as the interior of an aircraft, aft of the cockpit.
- The Aircraft Facility Checklist will be used for permanent SCIFs aboard aircraft.

The AO may determine that an Aircraft Facility Checklist may not be required for tactical SCIFs aboard aircraft if the following information is provided:

- Name of aircraft (tail number)/airborne T-SCIF
- Major command/organization
- ID number of parent SCIF, if applicable
- Location T-SCIF deployed from and date of deployment
- SCI compartment(s) involved in T-SCIF operations
- Time period for T-SCIF operation
- Name of exercise or operation
- Points of contact (responsible officers)
- Type of aircraft and area to be accredited as a T-SCIF
- Description of security measures for entire period of T-SCIF use (standard operating procedures)

Now we will discuss security requirements for Aircraft when Operating in Support of Missions involving SCI Material.

- Security Requirements for Aircraft when Operating in Support of Missions Involving SCI Material SCIF location shall be identified by aircraft tail number.
- Access to the aircraft interior shall be controlled at all times by SCI-indoctrinated personnel.
- There are no unique physical security construction standards for SCIFs aboard aircraft.
- Accreditation, such as that from the Defense Courier Service, is not required for aircraft used solely to transport SCI material between airfields.
- When all personnel on an aircraft are not briefed on every SCI compartment aboard, procedural methods or physical barriers shall be employed to isolate compartments of the SCI
- When an aircraft T-SCIF is no longer required, the responsible SCI security official shall conduct an inspection of the aircraft to ensure all SCI material has been removed

Additional Security Requirements for Stationary Aircraft

- The aircraft shall be parked within a controlled area that affords the greatest protection against surreptitious or forced entry

- In the absence of SCI-indoctrinated personnel, all SCI information shall be encrypted or removed and stored in an alternative accredited SCIF or location approved by the AO
- If the aircraft cannot be positioned within a U.S.-controlled area, the SCI is not encrypted, and removal of the SCI is not possible, then the following measures must be taken:
    - SCI-indoctrinated personnel shall remain with the aircraft
    - A guard force that can control the perimeter of the aircraft shall be deployed, unless infeasible
    - The guards shall possess U.S. SECRET clearances and be armed and equipped with emergency communication devices
- If the aircraft is located within a U.S.-controlled area, the SCI is not encrypted, and removal of SCI is not possible then, the following measures shall be taken:
    - The AO may mitigate the requirement for SCI-indoctrinated personnel provided the aircraft is equipped with, or stored within a structure equipped with, an intrusion detection system approved by the AO
    - All aircraft hatches and doors shall be secured with AO-approved locks and tamper-evident seals
    - A guard force must be available to respond to an alarm within five minutes
    - Guards shall possess U.S. SECRET clearances and be armed and equipped with emergency communication devices
    - If a cleared U.S. guard force is not available, the AO may approve other mitigation measures

NAVY T-SCIF SECURITY REQUIREMENTS

General Requirements for Naval T-SCIFS

- SCIFs on sub-surface vessels shall be accredited as T-SCIFs.
- T-SCIFs aboard a vessel include portable platforms or containers temporarily placed within ship space such as embarked Portable Shipboard Collection Vans.
- T-SCIFs shall be occupied by an SCI-indoctrinated person at all times unless the facility is protected by a GSA-approved lock, an approved intrusion detection system, and a response capability or other countermeasures approved by the AO.

Security Requirements for T-SCIFs

- Overall T-SCIF construction standards shall be the same as those used for permanent shipboard SCIFs.
- Vents, ducts, and similar openings shall be constructed to the same standards as those

used for a shipboard SCIF.

- The CTTA shall conduct a TEMPEST countermeasures inspection and shall recommend safeguards to limit compromising emanations. TEMPEST safeguards should be pre-engineered into platforms to the greatest extent possible.
- SCI materials shall be destroyed by means approved by the AO when no longer needed.
- AO-approved emergency destruction plans shall be rehearsed periodically by all personnel assigned to the T-SCIF and the rehearsals documented. 54 Chapter 6 Temporary, Airborne, and Shipboard SCIFs.
- Unclassified telecommunications shall meet the requirements for a shipboard SCIF, to the greatest extent practical.
- When the T-SCIF is no longer required, the responsible SCI security official shall conduct a closing inspection of the T-SCIF to ensure all SCI material has been removed.

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Five, T-SCIF Security Requirements. Now, let's test your comprehension of the material with a knowledge check. Select 'Next' to begin the knowledge check.

KNOWLEDGE CHECK 1

An Army T-SCIF shall be located within and area that affords the greatest degree of protection against surreptitious or forced entry when this happens?
Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐If a U.S.-controlled area or compound is not available
☐Whenever any T-SCIF is created
☐When surreptitious or forced entry is expected

KNOWLEDGE CHECK 2

This will be used for permanent SCIFs aboard aircraft.
Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐Secure Working Area Accreditation Form
☐The Aircraft Facility Checklist
☐SCI-indoctrinated Aircraft Authorization (S-IAA)

KNOWLEDGE CHECK 3

SCIFs on sub-surface vessels will not be accredited as T-SCIFs.

Select True or False, then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

LESSON 6: EXAMPLES OF T-SCIF CONFIGURATIONS

INTRODUCTION

This lesson will provide examples of T-SCIF configurations for the Army, Air Force, and Navy.

ARMY T-SCIF CONFIGURATIONS

In this section we will look at the three types of Army T-SCIFs. The T-SCIF may be established in a room, building, bunker, tent, truck-mounted or towed shelter, prefabricated modular trailer or building. Regardless of what configuration is adopted, it must provide appropriate acoustical, visual, and surreptitious entry protection. Based upon a local risk assessment, the approving authority may require additional physical security safeguards, i.e. the installation of sound-making devices (white noise generators), locks, access controls, alarms, or physical barriers like temporary walls, fences, radio frequency shielded shelter, etc. in order to prevent non-SCI indoctrinated personnel located in adjacent T-SCIF areas from gaining access either deliberate or unintentional to SCI information. An example of where this may be needed is a T-SCIF that is physically co-located within a collateral facility or a host nation installation.

SCIFs within a Division Tactical Operations Center (DTOC)

The T-SCIF is located within the boundaries of another facility but is isolated by the addition of a separate barrier. This might include a T-SCIF that was constructed within an existing building. If that building has previously been occupied by a non-U.S. element, you must request a TSCM. The Type of T-SCIF to be constructed depends on the location of the building, the positioning of the generators, positioning of physical security, and how the physical area can be controlled.

SCIFs Adjacent to a DTOC
The T-SCIF is located next to and adjacent to the boundaries of another facility, and has its own barrier.

Standalone T-SCIF
A ground-based T-SCIF could be located anywhere and the types of barriers need to be considered.

AIR FORCE T-SCIF OR SECURE WORK AREA (SWA)

The interior of all RC/WC-135 and EC130H aircraft, aft of the cockpit.

NAVAL T-SCIFS

Naval T-SCIF location can be at any designated point on a ship or submarine as long as the construction meets the same standards as those used for permanent shipboard SCIFs.

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Six, Examples of T-SCIF Configurations. Now, let's test your understanding of this lesson. Select 'Next' to begin the knowledge check.

KNOWLEDGE CHECK 1

A ground-based T-SCIF could be located anywhere.
Select True or False, then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

KNOWLEDGE CHECK 2

A SWA can be placed anywhere aboard an aircraft
Select True or False, then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

LESSON 7: SCI STORAGE & DESTRUCTION PROCEDURES

INTRODUCTION

This lesson will discuss SCI Storage and Destruction Procedures.

ARMY SCI STORAGE

Under field or combat conditions open storage of SCI media and materials requires a continuous presence by SCI-indoctrinated personnel.

Every effort shall be made to obtain from any available host command necessary support for the storage and protection of SCI, for example, security containers, generators, guards, weapons, etc. The quantity of SCI material within the T-SCIF shall be limited, to the extent possible, to an amount consistent with operational needs. All SCI shall be stored in GSA-approved security containers.

The AO may approve exceptions to the storage of SCI material in GSA-approved storage

containers for a specified period of time.

ARMY SCI DESTRUCTION PROCEDURES

SCI must be destroyed in a manner that will prevent reconstruction (i.e. burning, pulping, shredding, pulverizing, melting, and chemical decomposition). AIS and magnetic media must be destroyed in accordance with the NSA. The AO shall approve the means by which SCI material will be destroyed when it is no longer needed.

AIR FORCE SCI STORAGE & DESTRUCTION

Let's discuss Air Force SCI Storage and Destruction methods.

- SCI materials shall be encrypted or secured in an AO-approved security container
- If the aircraft is stationary, in the absence of SCI-indoctrinated personnel, all SCI information shall be encrypted or removed and stored in an alternative accredited SCIF or location approved by the AO
- Following an unscheduled landing in U.S.-controlled or non-hostile territory, the senior SCI-indoctrinated person shall retain control of the SCI material until approved storage arrangements can be effected through a local Special Security Officer or SCI indoctrinated official
- When no longer needed, SCI materials shall be destroyed by means approved by the AO
- Prior to an unscheduled landing in unfriendly or hostile territory, every reasonable effort shall be made to destroy unencrypted SCI material and communications security equipment in accordance with the emergency destruction plan
- Emergency destruction plans for SCI material shall be developed, approved by the AO, and rehearsed periodically by all personnel assigned to the aircraft; rehearsal results shall be documented

NAVY SCI STORAGE & DESTRUCTION

Finally, we'll discuss Navy SCI Storage and Destruction methods.

- SCI material shall be stored in a GSA-approved security container that is welded or otherwise permanently secured to the structural deck
- When no longer needed, SCI materials shall be destroyed by means approved by the AO
- AO-approved emergency destruction and evacuation plans shall be developed and rehearsed periodically by all personnel assigned to the SCIF and the rehearsals shall be documented

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Seven, SCI Storage and Destruction. Now, participate in a knowledge check to test your comprehension of the material. Please select 'Next' to begin.

KNOWLEDGE CHECK 1

The quantity of SCI material within a T-SCIF shall be limited, to the extent possible, to an amount consistent with operational needs.
Select True or False, then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

KNOWLEDGE CHECK 2

Air Force SCI materials can only be secured by being placed in an AO-approved security container.

Select True or False, then check your answers in the Answer Key at the end of this Student Guide.

☐True
☐False

LESSON 8: T-SCIF EMERGENCY ACTION PLAN

INTRODUCTION

This section covers how to create a T-SCIF Emergency Action Plan (EAP).

EAP-OVERVIEW

Each T-SCIF will establish and maintain an Emergency Action Plan that accounts for:

- Fire
- Natural disasters (i.e. floods, hurricanes)
- Combat Conditions during times of war
- Communication outages
- Entrance of emergency personnel (e.g., host country police and firemen) into the SCIF
- Physical protection and safety of those working in T-SCIFs

We never know what sort of emergency can befall them. Only that it is highly likely that sooner or later, something will happen. That is why the EAP is a critical component of any TSCIF - or

any other installation for that matter.

EAP-PLANNING

EAP Planning should address the following:

- Protection of persons and SCI
- Emergency Response Personnel
- Evacuation plans for persons and SCI
- Destruction of SCI when evacuation is not possible

EAP-TORNADOES

Tornadoes can strike with little or no warning and cause extensive damage to property as well as cause loss of life.

This debris littering a housing community shows the damage two days after the tornado struck the area.

EAP-HURRICANES

This was Hurricane Katrina. The water flooded New Orleans following breaking of the levees surrounding the city. Unfortunately, the Emergency Action Plan in place never anticipated such a complete disaster.

EAP-THE USE OF SANDBAGS

Members of the Army National Guard assist in the filling and placing of sandbags in areas affected by flooding of the White River in eastern Arkansas. Be prepared, and follow the EAP!

EAP-FOR SNOWSTORMS

Members of the Army National Guard walk to an aircraft during a snowstorm. Emergencies don't take a holiday.

EAP-FOR BLIZZARD CONDITIONS

An Emergency Action Plan has to cover all types of situations. Soldiers preparing for blizzard conditions follow their emergency plan procedure to protect structures from the dangers caused by sustained high winds and excessive snow fall.

EAP-FOR SIMULATED GAS LEAK & RADIATION

Emergency Action Plans must be practiced! Firefighters from the Couva South Fire Station check for gas leaks and radiation before search and rescue personnel enter a simulated collapse of a 3-story building where 15 people are trapped.

EAP-FOR SIMULATED BUILDING COLLAPSE

Here's another part of that same practice session. Search and rescue personnel with the Trinidad and Tobago fire department assist a mock victim of a simulated building collapse during a training exercise.

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Eight, T-SCIF Emergency Action Plan (EAP). Now, let's test your grasp of this lesson's material. Select 'Next' to begin the knowledge check.

KNOWLEDGE CHECK 1

A T-SCIF does not need to establish and maintain an Emergency Action Plan that accounts for which of the following?

Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐Fire
☐Natural Disaster (i.e., floods, hurricanes)
☐Communication Outages
☐Change in Leadership

KNOWLEDGE CHECK 2

EAP Planning should address which of the following

Select all that apply, then check your answers in the Answer Key at the end of this Student Guide.

☐Emergency Response Personnel
☐Protection of Persons and Special Access Programs (SAP)
☐Evacuation Plans for Persons and SCI
☐Destruction of SCI when evacuation is not possible

LESSON 9: SECURITY INCIDENTS, VIOLATIONS & INFRACTIONS

INTRODUCTION

By the end of this section you should be able to locate the guidance to:

- Properly Report Security Incidents
- Create a preliminary inquiry report
- Complete a damage assessment
- Review an investigation report for completeness

SECURITY INCIDENTS OVERVIEW

Security incidents are categorized as either Violations or Infractions. It is the responsibility of all SCI indoctrinated personnel to do the following:

- Report any security incidents affecting or involving SCI to the appropriate SSO or SCI Security Official
- Prepare an appropriate report that provides sufficient information to explain the incident.

SECURITY VIOLATIONS

A security violation involves:

- Any action that results in or could reasonably be expected to result in an unauthorized disclosure or compromise of classified information (including national intelligence)
- Any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of Executive Order 13526, or its implementing directives
- Any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of Executive Order 13526 or
- Any knowing, willful, or negligent action that attempts to contravene or violate any other provision of EO 13526 or its implementing directives

SECURITY VIOLATIONS-EXAMPLES

Security violations can be a result of many incidents. Loss or exposure of SCI require immediate reporting, an investigation, and a damage assessment describing the impact on national security.

Some of these incidents include, but are not limited to:

- Deliberate or accidental exposure of SCI resulting from loss
- Loss, theft, or capture
- Recovery by salvage
- Defection
- Press leaks or public declarations
- Release of unauthorized publications
- Discovery of clandestine surveillance and listening devices
- Loss that could reveal intelligence sources and methods
- Other unauthorized means

SECURITY INFRACTIONS

As mentioned in the security overview, security incidents fall into two distinct categories:

infractions and violations.

An Infraction is a security incident involving a deviation from current governing security regulations that does not result in an unauthorized disclosure or compromise of national intelligence information nor otherwise constitute an unauthorized disclosure or compromise of national intelligence information nor otherwise constitute a security violation (Previously "Practices Dangerous to Security").

An infraction requires immediate corrective action, but does not require investigation and does not constitute a security violation, but can lead to security violations or compromises if left uncorrected.

SECURITY INFRACTIONS-EXAMPLES

Examples of infractions include, but are not limited to:

- A courier who is carrying classified documents stopping at a public establishment to conduct personal business
- An employee placing burn bags adjacent to unclassified trash containers
- Personnel failing to change security container combinations as required

With all reported infractions, management officials will ensure prompt corrective action is taken and that those actions are documented.

REPORTING SECURITY INCIDENTS

Report all security incidents to an SCI security official in the following manner:
Incidents where SCI is compromised as a result of espionage or suspected espionage will be reported immediately by the most secure means to the appropriate HICE or designee.

Activity concerning the violation will cease pending a counterintelligence assessment by the appropriate HICE or designee.

SECURITY INCIDENTS-COMPROMISE CERTAIN

For a security violation with a determination of "Compromise Certain" the cognizant HICE will immediately report the incident to the appropriate Intelligence Community program manager.

The steps to this procedure are to first send a copy of the report to SSO Defense Intelligence Agency (DIA) Deputy Director for Mission Services, Counterintelligence and Security Office (DIA/DAC-3D).

Next, an investigation will be conducted to identify full details of the violation/compromise, and to determine what specific information was involved, what damage resulted, and whether culpability was involved in the incident.

SECURITY INCIDENTS-SUMMARY REPORTS

HICEs will provide summaries of investigations to the DNI and a copy to SSO DIA/DAC-3D under the following conditions:

When investigations show that SCI was inadvertently disclosed to foreign nationals or deliberately disclosed to unauthorized persons

- When cases under investigation involve espionage, flagrant dereliction of security duties, or serious inadequacies of security policies or procedures, local SCI security officials will advise the parent command SCI security officials of SCI security violations that occur within their security cognizance and involve personnel assigned to that parent command

SECURITY INCIDENTS-OUTSIDE THE AOR

If a security violation is committed by an activity that does not belong to the organization exercising security cognizance where the violation occurred, procedures are as follows:

- The SSO notifies both organizations of the security violation
- The organization with security cognizance ensures that an investigation is conducted
- A report of investigation is forwarded to both organizations
- The organization whose activity committed the violation will determine what corrective action should be taken
- The report of this determination will be forwarded to the other organization involved

SECURITY INCIDENTS-INFORMATION SYSTEMS

- All security violations occurring on computer systems, terminals, or equipment which process SCI will be reported through command SCI channels
- SCI security officials and the DODIIS site Information Assurance Manager will coordinate security incidents involving SCI systems
- Examples of serious incidents on a SCI network include, but are not limited to:
- Human error in reviewing media for content and classification, resulting in compromise
- Incorrect setting of a security filter that results in the compromise of intelligence

SECURITY INCIDENTS-IS INTRUSION ATEMPTS

Intrusion attempts, can be either physical, through

- Hacking
- Virus attacks
- Failure of a system or network security feature

NOTE: Commanders, supervisors, and their security managers must ensure that SCI security

violations or other information that could impact on an individual's continued eligibility for access to SCI are reported to the appropriate Central Adjudication Authority.

PRELIMINARY REPORT OF INQUIRY

When the SCI security official determines that a security violation has occurred,

- The SCI security official *must report the violation within 72 hours of discovery* to the appropriate HICE/SIO with information copies to SSO DIA/DAC-3D
- The local SIO must ensure the appointment of an inquiry official
- Preliminary Inquiries *will not* be conducted by the SSO or staff member
- In addition, classify the notification according to content, but at least Confidential, to prevent further possible disclosure. Send the notification by priority Defense Special Security Communication System (DSSCS) message or other secure channel.

SECURITY VIOLATION-INVESTIGATION REPORT

Reports of investigation will include sufficient detail to explain the incident.

The report will assess intent, location of incident, risk of compromise, sensitivity of information, and mitigating factors in arriving at a final analysis of the incident.

DAMAGE ASSESSMENT OF COMPROMISED INFORMATION

Be aware that loss or exposure of SCI from any cause requires immediate:

- Reporting
- Investigation and
- Submission of a damage assessment describing the impact on national security

The original classification authority (OCA) must:

- Re-evaluate lost or compromised information
- Determine if a change in classification is needed
- Indicate damage to national security

KNOWLEDGE CHECKS

KNOWLEDGE CHECK INTRODUCTION

You have completed Lesson Nine, Security Incidents, Violations, and Infractions. Now, let's check your command of the material. Select 'Next' to begin the knowledge check.

KNOWLEDGE CHECK 1

SCI security officials must report security violations within how many hours of discovery to the appropriate HICE/SIO

Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐24 hours
☐36 hours
☐48 hours
☐72 hours

KNOWLEDGE CHECK 2

Any action that results in or could reasonably be expected to result in an unauthorized disclosure or compromise of classified information (including national intelligence), is considered a what?

Select the best answer, then check your answers in the Answer Key at the end of this Student Guide.

☐Security Infraction
☐Security Disturbance
☐Security Transgression
☐Security Violation

LESSON 10: T-SCIF COURSE CONCLUSION

SUMMARY

Congratulations! You have completed the T-SCIF course. You should now be able to:

- Define Sensitive Compartmented Information, or SCI, and T-SCIF
- Recognize National Security Policy and SCI Authorities
- Identify SCI Leadership Responsibilities
- Identify Required Documentation for T-SCIF
- Explain T-SCIF Security Requirements
- Describe Examples of T-SCIF Configurations
- Discuss how SCI is Stored and Destroyed
- Create a T-SCIF Emergency Action Plan (EAP)
- Properly Report Security Incidents & Violations

Please select Exit, and proceed to STEPP to take the exam.

APPENDIX A: KNOWLEDGE CHECK ANSWER KEY

LESSON 1 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

SCI is classified national intelligence concerning, or derived from, intelligence sources, methods of analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

☒True (Correct answer)
☐False

Feedback: You are correct! SCI is classified national intelligence concerning, or derived from, intelligence sources, methods, or analytical processes that is required to be protected within formal access control systems established and overseen by the Director of National Intelligence.

LESSON 2 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

What identifies DIA Counterintelligence and Security Office (DAC), as the sole accrediting authority for DOD SCI Facilities?

☐ICD 700
☒DODM 5105.21, Vol. 2 (Correct answer)
☐EO 12333, as amended

Feedback: That's right! DODM 5105.21, Vol. 2 Identifies the DIA Counterintelligence and Security Office (DAC), as the sole accrediting authority for DOD SCI Facilities.

KNOWLEDGE CHECK 2

Which of the following establishes control over SCI?

☒EO 13470 (Correct Answer)
☐EO 12333, as amended
☐DODM 5105.21, Vol.2
☐ICD 700
☐DODI 5200.01

Feedback: That's right! EO 13470 establishes control over SCI.

LESSON 3 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

All personnel assigned to the position of SSO will attend the SCI Security Officials course within how many days of being appointed?

☐30 days

☐60 days

☒120 days (Correct Answer)

Feedback: You are correct! All personnel assigned to the position of SSO will attend the SCI Security Officials course within 120 days of being appointed to these security duties.

KNOWLEDGE CHECK 2

Who administers uniform DOD SCI policy for Physical Security and Information Security?

☒Director of DIA (Correct Answer)

☐Head of Intelligence Community Element

☐Cognizant Security Authority

Feedback: You are correct! The Director of DIA administers uniform DOD SCI policy for Physical Security and Information Security

LESSON 4 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

The Army T-SCIF Request must be submitted at least how many days prior to T-SCIF activities?

☐7 days

☒14 days (Correct Answer)

☐21 days

Feedback: That's right! The Army T-SCIF Request must be submitted at least 14 days prior to T-SCIF activation.

KNOWLEDGE CHECK 2

Appointment letters are required for both Air Force and Navy T-SCIFs

☒True (Correct Answer)

☐False

Feedback: That's right! You selected the correct response.

LESSON 5 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

An Army T-SCIF shall be located within and area that affords the greatest degree of protection against surreptitious or forced entry when this happens?

☒If a U.S.-controlled area or compound is not available (Correct Answer)
☐Whenever any T-SCIF is created
☐When surreptitious or forced entry is expected

Feedback: You are correct! An Army T-SCIF shall be located within an area that affords the greatest degree of protection against surreptitious or forced entry if a U.S.-controlled area or compound is not available.

KNOWLEDGE CHECK 2

This will be used for permanent SCIFs aboard aircraft.

☐Secure Working Area Accreditation Form
☒The Aircraft Facility Checklist (Correct Answer)
☐SCI-indoctrinated Aircraft Authorization (S-IAA)

Feedback: You are correct! An Aircraft Facility Checklist will be used for permanent SCIFs aboard aircraft.

KNOWLEDGE CHECK 3

SCIFs on sub-surface vessels will not be accredited as T-SCIFs

☐True
☒False (Correct Answer)

Feedback: You are correct! SCIFs on sub-surface vessels will be accredited as T-SCIFs.

LESSON 6 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

A ground-based T-SCIF could be located anywhere

☒True (Correct Answer)
☐False

Feedback: That's right! A ground-based T-SCIF could be located anywhere.

KNOWLEDGE CHECK 2

A SWA can be placed anywhere aboard an aircraft.

☐True

☒False (Correct Answer)

Feedback: That's right! A SWA cannot be placed anywhere aboard an aircraft, only aft the cockpit.

LESSON 7 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

The quantity of SCI material within a T-SCIF shall be limited, to the extent possible, to an amount consistent with operational needs.

☒True (Correct Answer)

☐False

Feedback: You are correct! The quantity of SCI material within a T-SCIF shall be limited, to the extent possible, to an amount consistent with operational needs.

KNOWLEDGE CHECK 2

Air Force SCI materials can only be secured by being placed in an AO approved security container.

☐True

☐False (Correct Answer)

Feedback: You are correct! Air Force SCI materials shall be encrypted or secured in an AO-approved security container.

LESSON 8 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

A T-SCIF does not need to establish and maintain an Emergency Action Plan that accounts for which of the following?

☐Fire

☐Natural Disaster (i.e., floods, hurricanes)

☐Communication Outages

☒Change in Leadership (Correct Answer)

Feedback: That's right! A T-SCIF does not need to establish and maintain an Emergency Action Plan that accounts for a change in leadership.

KNOWLEDGE CHECK 2

EAP Planning should address which of the following

☒Emergency Response Personnel (Correct Answer 1 of 3)

☐Protection of Persons and Special Access Programs (SAP)
☒Evacuation Plans for Persons and SCI (Correct Answer 2 of 3)
☒Destruction of SCI when evacuation is not possible (Correct Answer 3 of 3)

Feedback: That's right! EAP should address Emergency Response Personnel, Evacuation Plans for Persons and SCI, and Destruction of SCI when evacuation is not possible.

LESSON 9 KNOWLEDGE CHECK

KNOWLEDGE CHECK 1

SCI security officials must report security violations within how many hours of discovery to the appropriate HICE/SIO

☐24 hours
☐36 hours
☐48 hours
☒72 hours (Correct Answer)

Feedback: You are correct! SCI security officials must report security violations within 72 hours of discovery to the appropriate HICE/SIO.

KNOWLEDGE CHECK 2

Any action that results in or could reasonably be expected to result in an unauthorized disclosure or compromise of classified information (including national intelligence), is considered a what?

☐Security Infraction
☐Security Disturbance
☐Security Transgression
☒Security Violation (Correct Answer)

Feedback: You are correct! Any action that results in or could reasonably be expected to result in an unauthorized disclosure or compromise of classified information (including national intelligence), is considered a Security Violation.