Fixed Facility Checklist Short

Student Guide

April 2025

Center for Development of Security Excellence

Contents

Introduction

Special Access Program (SAP) security professionals, like yourself, have the responsibility of ensuring the security of designated Special Access Program Facilities, or SAPFs. One way to do this is through the use of specific processes and tools, such as the Fixed Facility Checklist (FFC). The FFC is utilized throughout the lifecycle of the SAPF to ensure it meets all accreditation requirements from preconstruction to final accreditation. The FFC documents changes to the SAPF to ensure compliance with the processes outlined in DOD Manual (DODM) 5205.07 and the National Counterintelligence and Security Center (NCSC) “Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities” (NCSC SCIF Specifications). The NCSC SCIF Specifications are commonly referred to as the ICD 705 Tech Spec.

There are specific actions required of you and other SAP security professionals to complete the FFC with accuracy and fidelity. In this Short, we will walk through the sections of the FFC in detail so that you will be able to indicate appropriate actions for completing the FFC for a SAPF. Although the FFC is also used for the establishment of Sensitive Compartmented Information Facilities (SCIFs) this Short will focus on SAP processes.

Note that this Short may also benefit non-SAP personnel, with the understanding that some roles and responsibilities will be different.

Policies

To complete the FFC with accuracy, you need to be aware of the policies that provide guidance for physical security and construction requirements of SAPFs.

DODM 5205.07 provides physical security procedures for Department of Defense SAPs. This includes requirements for SAP FFCs.

The NCSC Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Chapter 3, states the requirements of fixed facility SCIFs for FFC documentation. This includes construction requirements detailed in the FFC. Use these policies as a reference as you complete the FFC. Remember as previously mentioned that although the NCSC SCIF Specifications policy is written for SCIFs, it is leveraged as the physical security standards for DOD SAPFs.

Roles and Responsibilities

Several roles contribute to and are responsible for the security of SAPFs.

The Program Security Officer (PSO), Government SAP Security Officer (GSSO), and the Contractor Special Security Officer (CSSO), are all responsible for the daily operation of the facility.

- The PSO is the government security professional responsible for all aspects of SAP security.
- The GSSO and CSSO provide hands-on security administration and management at the facility level. Their roles apply to both government facilities and contractor facilities.

The SAPF Accrediting Official (SAPF-AO) has a physical security role in protecting facilities and spaces used to preview and protect unauthorized access to SAP information.

The Certified TEMPEST Technical Authority (CTTA) is an experienced technically qualified government employee who meets established certification requirements. The CTTA ensures the facility meets TEMPEST requirements. Individuals in these roles work together to ensure SAP areas are fully secured and meet standards for security that affect accreditation and classification of information. The term TEMPEST refers to electronic emanations and will be covered later in this Short.

SAPF-AO

It's the responsibility of the SAPF-AO to inspect any SAP area before accreditation. The SAPF-AO conducts periodic re-inspections based on threat, physical modifications, sensitivity of SAPs, and past security performance. Re-inspections occur at least every three years. They may occur at any time, announced or unannounced. The SAPF-AO reviews the FFC during inspections to ensure compliance.

PSO/GSSO/CSSO

As a part of overseeing daily security operations, the PSO, GSSO, and CSSO are also responsible for notifying the SAPF-AO of any activity that affects accreditation. Additionally, the PSO validates facility security clearances (FCLs) as required for DOD contractors under the National Industrial Security Program (NISP). Where applicable, the CSSO must notify the PSO of any activity that affects the FCL, as the classification level of the SAP information cannot exceed the classification level of the FCL. Similarly, the CSSO must also report anything that affects SAP accreditation. Facilities must be accredited before receiving generating, processing, using, or storing SAP classified information.

CTTA

CTTAs are responsible for reviewing the TEMPEST checklist. They assess requirements to prevent electronic emanations, and recommend countermeasures based on emanations tests.

FFC Overview

Just as each role plays an important part in securing a SAPF, each section of the FFC does too. Before we take a closer look at the FFC, let's preview its nine main sections.

- Section A is for general information.
- Section B is a more detailed Security-in-Depth.
- Section C is for information about SAPF Security.
- Section D is where you include information about SAPF Doors.
- Section E details the Intrusion Detection Systems, or IDS, of the SAPF.
- Section F is where you record information about Telecommunication Systems and Equipment Baseline.
- Section G is for information regarding Acoustical Protection.
- Section H is for Classified Destruction Methods.
- Finally, section I is where you record details about Information Systems, TEMPEST, and Technical Security. It's important to regard and treat the FFC as a living document. You're expected to update the FFC and its sections when any changes occur in the facility.

Because we are focusing on SAPFs, we've replaced references for SCIF with SAPF in applicable areas.

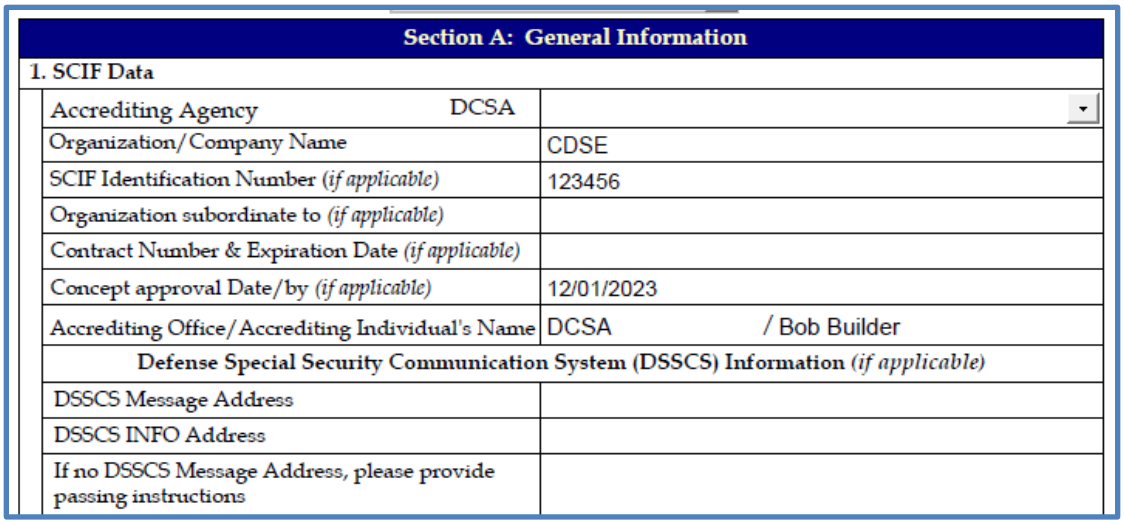
Please note when you complete the FFC for a SAPF, you will also replace SCIF with SAPF in all cases. As you walk through each section of the FFC, review the actions you take to complete the form.

Section A: General Information

The first section you encounter on the FFC is Section A. Section A is where you record general information and identifiable data about the SAPF. This includes describing facility-specific data; identifying the exact location and mailing address; responsible security personnel; and noting accreditation data and the status of construction and inspections.

Data

Take a moment to review subsection 1: Data.



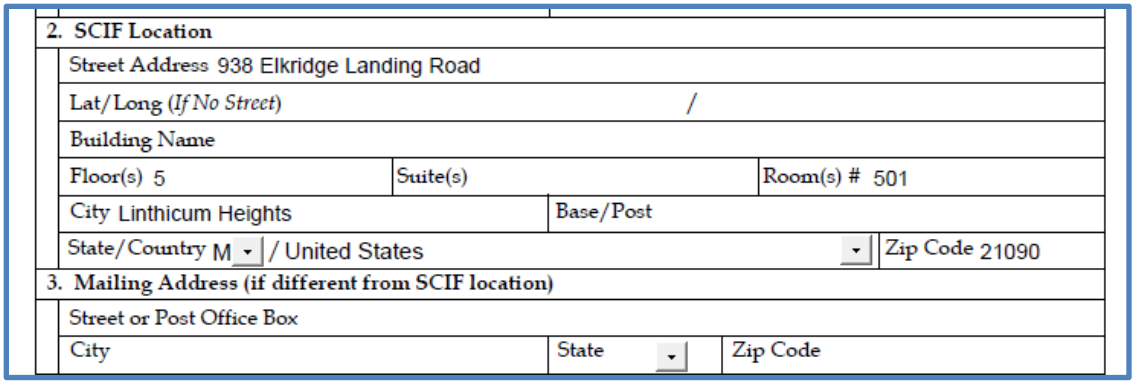
Section A: General Information	
1. SCIF Data	
Accrediting Agency DCSA	
Organization/Company Name	CDSE
SCIF Identification Number *(if applicable)*	123456
Organization subordinate to *(if applicable)*	
Contract Number & Expiration Date *(if applicable)*	
Concept approval Date/by *(if applicable)*	12/01/2023
Accrediting Office/Accrediting Individual's Name	DCSA / Bob Builder
Defense Special Security Communication System (DSSCS) Information *(if applicable)*	
DSSCS Message Address	
DSSCS INFO Address	
If no DSSCS Message Address, please provide passing instructions	

Information Requested	Information Input
Accrediting Agency	List the agency providing the accreditation. In the example, this is listed as DCSA.
Organization/Company Name	List the organization which hosts the SCIF/SAPF. In the example, this is listed as CDSE.
SCIF Identification Number *(if applicable)*	List the SCIF/SAPF Identification Number. If required, the **SAPF Identification Number** can be obtained from the SAPF-AO. If this is a modification, it may be found on a current accreditation letter. Note that this field is required for SCIFs, and this process would be routed through your Special Security Officer (SSO).
Organization subordinate to *(if applicable)*	List the organization that the organization being reviewed is subordinate to, if applicable.
Contract Number & Expiration Date *(if applicable)*	List the contract number and expiration date, if applicable.
Concept approval Date/by *(if applicable)*	List the concept approval date, if applicable. In the example, this is listed as 12/01/2023.
Accrediting Office/Accrediting Individual's Name	List the accrediting office and individual who is responsible for accrediting the facility. In the example this is listed as DCSA/Bob Builder.
Defense Special Security Communication System (DSSCS) Information *(if applicable)*	This is a section header.
DSSCS Message Address	List the DSSCS Message address, if applicable.
DSSCS INFO Address	List the DSSCS INFO address, if applicable.

If no DSSCS Message Address, please provide passing instructions	Include instructions for passing the information to DSSCS, if applicable.

Location and Mailing Address

Review subsections 2 and 3: Location and Mailing Address.

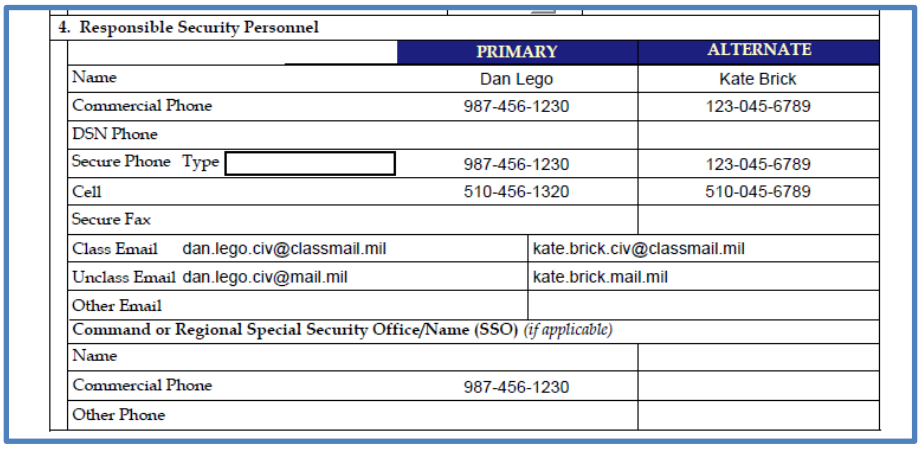


2. SCIF Location			
Street Address 938 Elkridge Landing Road			
Lat/Long (*If No Street*) /			
Building Name			
Floor(s) 5	Suite(s)	Room(s) # 501	
City Linthicum Heights	Base/Post		
State/Country M / United States		Zip Code 21090	
3. Mailing Address (if different from SCIF location)			
Street or Post Office Box			
City	State	Zip Code	

Subsection	Important Information
2. SCIF Location	Enter the physical address of the SAPF in the **SCIF Location** field..
3. Mailing Address (if different from SCIF location)	Record the mailing address, if different from the physical address, in the **Mailing Address** field.

Responsible Security Personnel

Review subsection 4: Responsible Security Personnel.

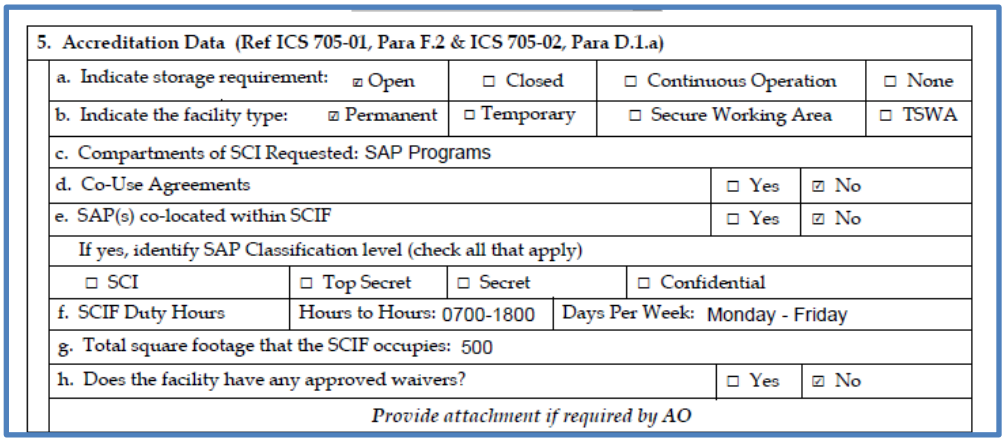


4. Responsible Security Personnel	PRIMARY	ALTERNATE
Name	Dan Lego	Kate Brick
Commercial Phone	987-456-1230	123-045-6789
DSN Phone		
Secure Phone Type	987-456-1230	123-045-6789
Cell	510-456-1320	510-045-6789
Secure Fax		
Class Email dan.lego.civ@classmail.mil	kate.brick.civ@classmail.mil	
Unclass Email dan.lego.civ@mail.mil	kate.brick.mail.mil	
Other Email		
Command or Regional Special Security Office/Name (SSO) *(if applicable)*		
Name		
Commercial Phone	987-456-1230	
Other Phone		

Subsection	Important Information
4. Responsible Security Personnel	In the **Responsible Security Personnel** subsection, you provide the information on the primary CSSO/GSSO for the facility and list an alternate.

Accreditation Data

Now, review the information for subsection 5: Accreditation Data.

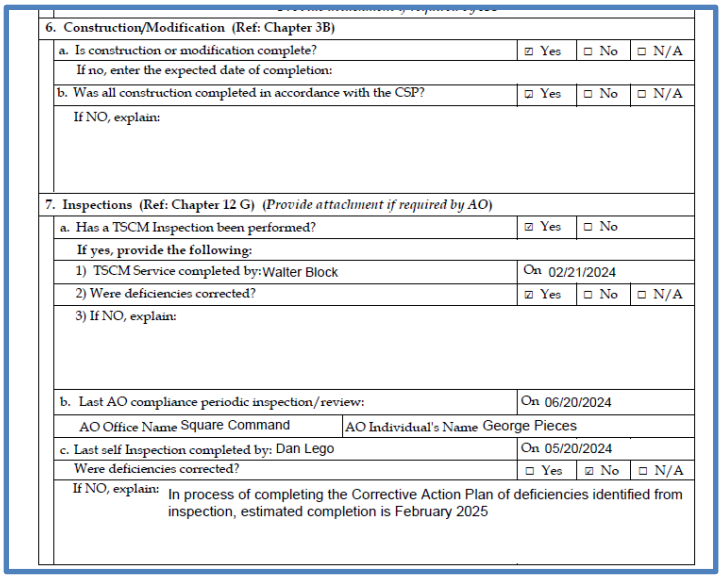


5. Accreditation Data (Ref ICS 705-01, Para F.2 & ICS 705-02, Para D.1.a)				
a. Indicate storage requirement: ☑ Open	☐ Closed	☐ Continuous Operation	☐ None	
b. Indicate the facility type: ☑ Permanent	☐ Temporary	☐ Secure Working Area	☐ TSWA	
c. Compartments of SCI Requested: SAP Programs				
d. Co-Use Agreements			☐ Yes	☑ No
e. SAP(s) co-located within SCIF			☐ Yes	☑ No
If yes, identify SAP Classification level (check all that apply)				
☐ SCI	☐ Top Secret	☐ Secret	☐ Confidential	
f. SCIF Duty Hours	Hours to Hours: 0700-1800	Days Per Week: Monday - Friday		
g. Total square footage that the SCIF occupies: 500				
h. Does the facility have any approved waivers?			☐ Yes	☑ No
Provide attachment if required by AO				

Subsection	Important Information
5. a. Indicate storage requirement	Under the **Accreditation Data** subsection, you indicate the storage requirement such as Open, Closed, or Continuous.
5. b. through d.	You also indicate the facility type, such as Permanent, Temporary, Secure Working Area, or Temporary Secure Working Area (TSWA), and any co-use agreements.

Construction/Modifications and Inspections

Review subsections 6 and 7: Construction/Modification, and Inspections.



6. Construction/Modification (Ref: Chapter 3B)				
a. Is construction or modification complete?		☑ Yes	☐ No	☐ N/A
If no, enter the expected date of completion:				
b. Was all construction completed in accordance with the CSP?		☑ Yes	☐ No	☐ N/A
If NO, explain:				
7. Inspections (Ref: Chapter 12 G) (*Provide attachment if required by AO*)				
a. Has a TSCM Inspection been performed?		☑ Yes	☐ No	
If yes, provide the following:				
1) TSCM Service completed by: Walter Block		On 02/21/2024		
2) Were deficiencies corrected?		☑ Yes	☐ No	☐ N/A
3) If NO, explain:				
b. Last AO compliance periodic inspection/review:		On 06/20/2024		
AO Office Name Square Command	AO Individual's Name George Pieces			
c. Last self Inspection completed by: Dan Lego		On 05/20/2024		
Were deficiencies corrected?		☐ Yes	☑ No	☐ N/A
If NO, explain: In process of completing the Corrective Action Plan of deficiencies identified from inspection, estimated completion is February 2025				

Subsection	Important Information
6. Construction/Modification (Ref: Chapter 3B)	State the status of construction or any modifications in the **Construction/Modification** subsection.
7. Inspections (Ref: Chapter 12 G) *(Provide attachment if required by AO)*	For the **Inspections** subsection, include information on Technical Surveillance Counter Measure (TSCM), Physical, or Staff Assistance Visits (SAVs).

Section B: Security-in-Depth

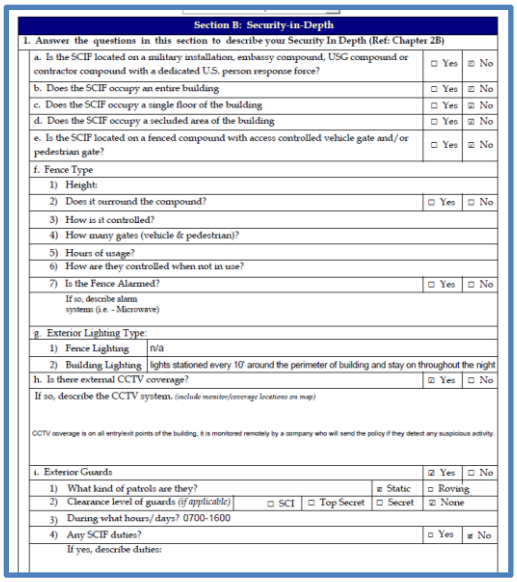
SAPF-AOs are responsible for determining if a facility's security program meets security requirements. Section B is where you record details to help the SAPF-AO make a determination about the Security-in-Depth (SID).

SID is a determination made by the SAPF-AO that a facility's security program consists of layered and complementary security controls that are sufficient to deter and detect unauthorized entry and movement.

Layers in this model include strategic leveled measures of security, starting with exterior perimeters and guard patrols, to interior protections such as alarm systems and controlled access. Section B includes subsections differentiated by both exterior and interior information.

Security-in-Depth

Review subsection 1: Security-in-Depth.



Section B: Security-in-Depth

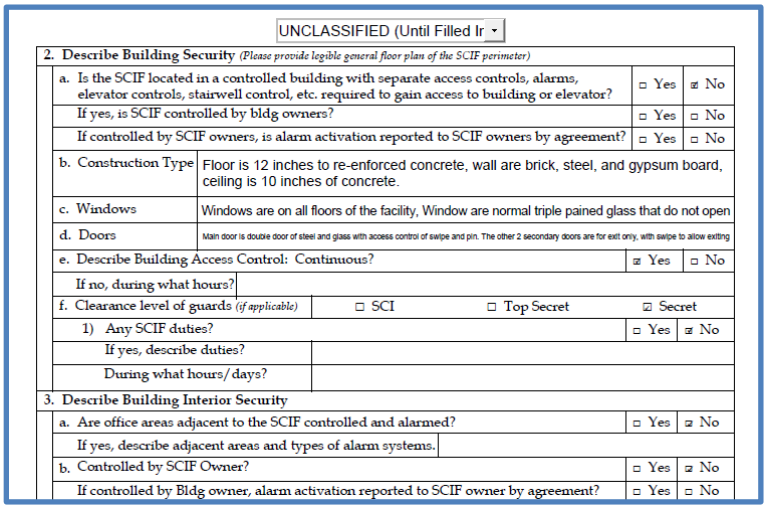
1. Answer the questions in this section to describe your Security In Depth (Ref: Chapter 2B)

a. Is the SCIF located on a military installation, embassy compound, USG compound or contractor compound with a dedicated U.S. person response force?	☐ Yes	☒ No
b. Does the SCIF occupy an entire building	☐ Yes	☒ No
c. Does the SCIF occupy a single floor of the building	☐ Yes	☒ No
d. Does the SCIF occupy a secluded area of the building	☐ Yes	☒ No
e. Is the SCIF located on a fenced compound with access controlled vehicle gate and/or pedestrian gate?	☐ Yes	☒ No
f. Fence Type		
1) Height:		
2) Does it surround the compound?	☐ Yes	☐ No
3) How is it controlled?		
4) How many gates (vehicle & pedestrian)?		
5) Hours of usage?		
6) How are they controlled when not in use?		
7) Is the Fence Alarmed?	☐ Yes	☐ No
If so, describe alarm systems (i.e. - Microwave)		
g. Exterior Lighting Type:		
1) Fence Lighting: n/a		
2) Building Lighting: lights stationed every 10' around the perimeter of building and stay on throughout the night		
h. Is there external CCTV coverage?	☑ Yes	☐ No
If so, describe the CCTV system. *(include monitor/coverage locations on map)* CCTV coverage is on all entry/exit points of the building, it is monitored remotely by a company who will send the policy if they detect any suspicious activity.		
i. Exterior Guards	☑ Yes	☐ No
1) What kind of patrols are they?	☒ Static	☐ Roving
2) Clearance level of guards *(if applicable)* ☐ SCI ☐ Top Secret ☐ Secret	☑ None	
3) During what hours/days? 0700-1600		
4) Any SCIF duties?	☐ Yes	☒ No
If yes, describe duties:		

Subsection	Important Information
1. Answer the questions in this section to describe your Security-in-Depth (Ref: Chapter 2B)	In the **Security-in-Depth** subsection, you record information about the exterior of the building in which the SAPF is housed, paying close attention to layers in place that help provide SID.
	SID layers include the location, fence, exterior lighting, and static and roving guards.

Describe Building Security and Interior Security

Now review subsections 2 and 3: Describe Building Security and Describe Building Interior Security.



UNCLASSIFIED (Until Filled Ir

2. Describe Building Security *(Please provide legible general floor plan of the SCIF perimeter)*

a. Is the SCIF located in a controlled building with separate access controls, alarms, elevator controls, stairwell control, etc. required to gain access to building or elevator?		☐ Yes	☒ No
If yes, is SCIF controlled by bldg owners?		☐ Yes	☐ No
If controlled by SCIF owners, is alarm activation reported to SCIF owners by agreement?		☐ Yes	☐ No
b. Construction Type	Floor is 12 inches to re-enforced concrete, wall are brick, steel, and gypsum board, ceiling is 10 inches of concrete.		
c. Windows	Windows are on all floors of the facility, Window are normal triple pained glass that do not open		
d. Doors	Main door is double door of steel and glass with access control of swipe and pin. The other 2 secondary doors are for exit only, with swipe to allow exiting		
e. Describe Building Access Control: Continuous?		☒ Yes	☐ No
If no, during what hours?			
f. Clearance level of guards *(if applicable)*	☐ SCI ☐ Top Secret ☑ Secret		
1) Any SCIF duties?		☐ Yes	☒ No
If yes, describe duties?			
During what hours/days?			

3. Describe Building Interior Security

a. Are office areas adjacent to the SCIF controlled and alarmed?	☐ Yes	☒ No
If yes, describe adjacent areas and types of alarm systems.		
b. Controlled by SCIF Owner?	☐ Yes	☒ No
If controlled by Bldg owner, alarm activation reported to SCIF owner by agreement?	☐ Yes	☐ No

Subsection	Important Information
2. Describe Building Security *(Please provide legible general floor plan of the SCIF perimeter)*	**Describe Building Security** is a subsection where you provide information on the interior of the building in which the building is housed, including building construction, access control, and guards.
3. Describe Building Interior Security	**Describe Building Interior Security** is a subsection where you provide information specific to interior alarm systems.

Section C: SAPF Security

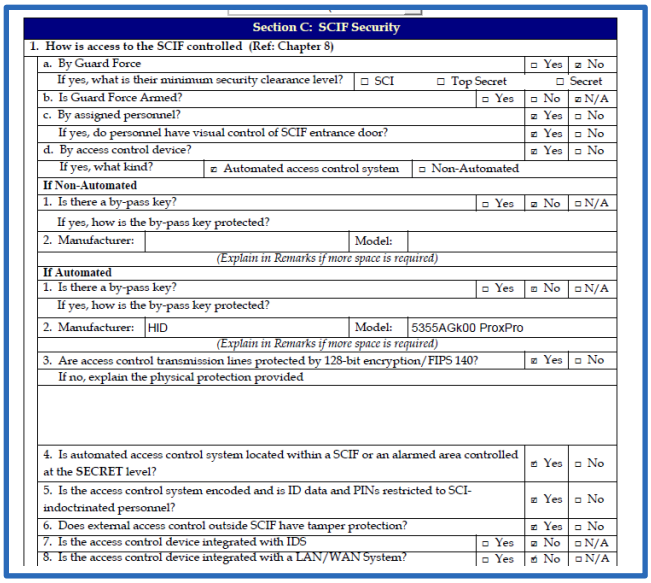
Section C of the FFC looks at the structural components related to access control.

In this section, you identify how individuals access the SAPF through any penetrable areas—including doors, windows, and ducts— and describe how the SAPF is constructed. When considered collectively, the penetrable areas detailed in this section help identify the potential vulnerabilities within the SAPF.

Note that you can find additional information on physical security construction of walls in the SAPF Wall Types Job Aid.

SAPF Access

Review subsection 1: SAPF Access.



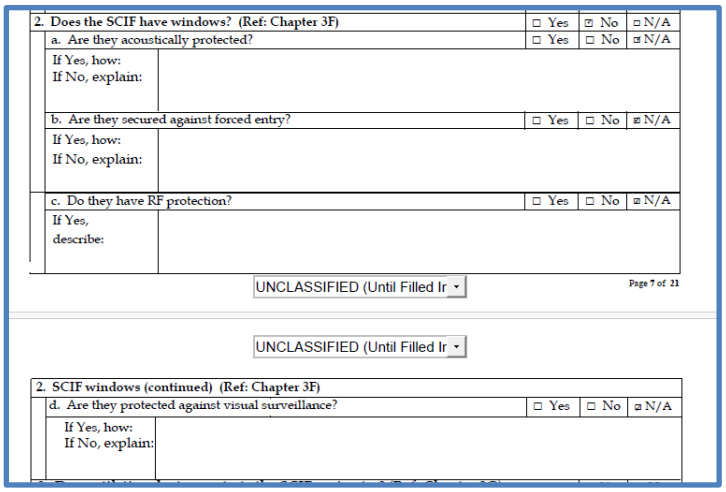
Section C: SCIF Security

1. How is access to the SCIF controlled (Ref: Chapter 8)			
a. By Guard Force		☐ Yes	☑ No
If yes, what is their minimum security clearance level?	☐ SCI ☐ Top Secret ☐ Secret		
b. Is Guard Force Armed?	☐ Yes	☐ No	☑ N/A
c. By assigned personnel?		☑ Yes	☐ No
If yes, do personnel have visual control of SCIF entrance door?		☑ Yes	☐ No
d. By access control device?		☑ Yes	☐ No
If yes, what kind?	☑ Automated access control system ☐ Non-Automated		
If Non-Automated			
1. Is there a by-pass key?	☐ Yes	☑ No	☐ N/A
If yes, how is the by-pass key protected?			
2. Manufacturer:	Model:		
(Explain in Remarks if more space is required)			
If Automated			
1. Is there a by-pass key?	☐ Yes	☑ No	☐ N/A
If yes, how is the by-pass key protected?			
2. Manufacturer: HID	Model: 5355AGk00 ProxPro		
(Explain in Remarks if more space is required)			
3. Are access control transmission lines protected by 128-bit encryption/FIPS 140?		☑ Yes	☐ No
If no, explain the physical protection provided			
4. Is automated access control system located within a SCIF or an alarmed area controlled at the SECRET level?		☑ Yes	☐ No
5. Is the access control system encoded and is ID data and PINs restricted to SCI-indoctrinated personnel?		☑ Yes	☐ No
6. Does external access control outside SCIF have tamper protection?		☑ Yes	☐ No
7. Is the access control device integrated with IDS	☐ Yes	☑ No	☐ N/A
8. Is the access control device integrated with a LAN/WAN System?	☐ Yes	☑ No	☐ N/A

Subsection	Important Information
1. How is access to the SCIF controlled (Ref: Chapter 8)	The **SAPF Access** subsection focuses on access control and requires information about how residents and visitors gain access to the facility by guard, non-automated, or automated means.

Windows

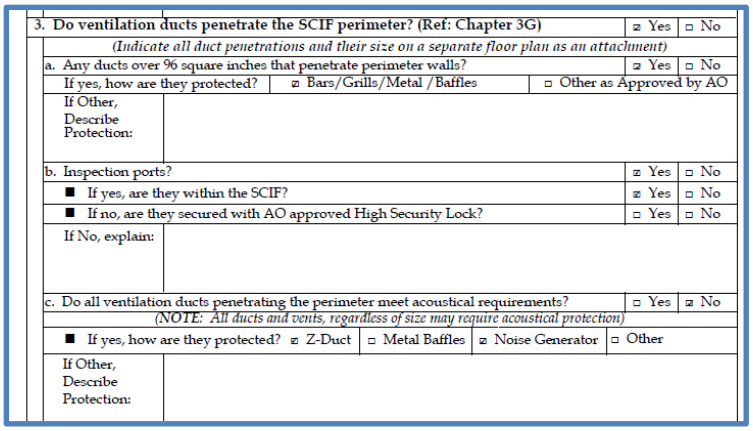
Now, review the information on subsection 2: Windows.



Subsection	Important Information
2. Does the SCIF have windows? (Ref: Chapter 3F)	The **Windows** subsection is where you provide information about how any existing windows are protected from acoustics, forced entry, radio frequency (RF), and/or visual surveillance.

Ducts

Review subsection 3: Ducts.

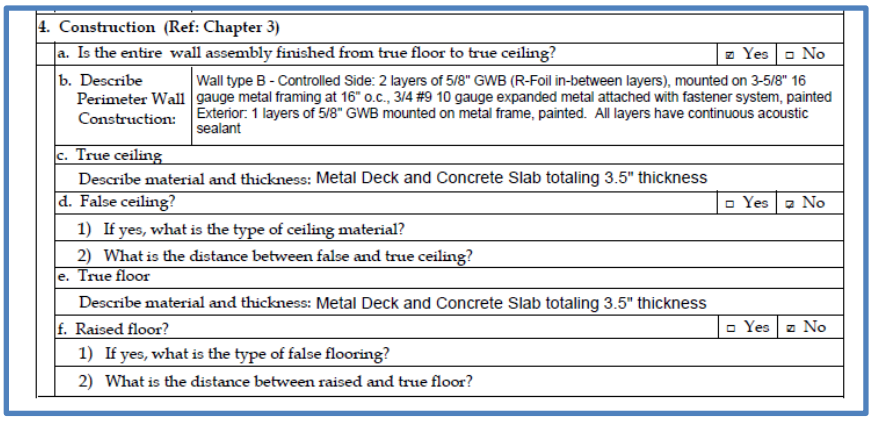


3. Do ventilation ducts penetrate the SCIF perimeter? (Ref: Chapter 3G)	☒ Yes	☐ No
(Indicate all duct penetrations and their size on a separate floor plan as an attachment)		
a. Any ducts over 96 square inches that penetrate perimeter walls?	☒ Yes	☐ No
If yes, how are they protected? ☒ Bars/Grills/Metal /Baffles ☐ Other as Approved by AO		
If Other, Describe Protection:		
b. Inspection ports?	☒ Yes	☐ No
■ If yes, are they within the SCIF?	☒ Yes	☐ No
■ If no, are they secured with AO approved High Security Lock?	☐ Yes	☐ No
If No, explain:		
c. Do all ventilation ducts penetrating the perimeter meet acoustical requirements?	☐ Yes	☒ No
(NOTE: All ducts and vents, regardless of size may require acoustical protection)		
■ If yes, how are they protected? ☒ Z-Duct ☐ Metal Baffles ☒ Noise Generator ☐ Other		
If Other, Describe Protection:		

Subsection	Important Information
3. Do ventilation ducts penetrate the SCIF perimeter? (Ref: Chapter 3G)	In the **Ventilation Duct** subsection, you provide information about duct work that may penetrate the perimeter of the SCIF.
	Include the size of penetration and methods to protect; inspection ports to observe defense measures; and acoustic requirements such as z-duct, metal baffles, and noise generators.

Construction

Review the fourth subsection: Construction.



4. Construction (Ref: Chapter 3)		
a. Is the entire wall assembly finished from true floor to true ceiling?	☒ Yes	☐ No
b. Describe Perimeter Wall Construction:	Wall type B - Controlled Side: 2 layers of 5/8" GWB (R-Foil in-between layers), mounted on 3-5/8" 16 gauge metal framing at 16" o.c., 3/4 #9 10 gauge expanded metal attached with fastener system, painted Exterior: 1 layers of 5/8" GWB mounted on metal frame, painted. All layers have continuous acoustic sealant	
c. True ceiling		
Describe material and thickness: Metal Deck and Concrete Slab totaling 3.5" thickness		
d. False ceiling?	☐ Yes	☒ No
1) If yes, what is the type of ceiling material?		
2) What is the distance between false and true ceiling?		
e. True floor		
Describe material and thickness: Metal Deck and Concrete Slab totaling 3.5" thickness		
f. Raised floor?	☐ Yes	☒ No
1) If yes, what is the type of false flooring?		
2) What is the distance between raised and true floor?		

Subsection	Important Information
4. Construction (Ref: Chapter 3)	In the **Construction** subsection you include details about the wall, ceiling, and floor construction.
Questions c. through f. regarding true/false ceiling and true/false floor.	Note that “true” means the actual floor or ceiling, and “false” means an additional floor or ceiling that is used in a space, such as floor or ceiling tiles.

Knowledge Check

Consider what you learned about Section C of the FFC and answer the question.

Sam is evaluating a SAPF and is completing Section C (SAPF Security) of the FFC. Sam is inspecting the construction of the ceiling and notices the use of ceiling tiles in the SAPF. Which of the following statements correctly indicates how Sam should note the use of ceiling tiles on the FFC?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

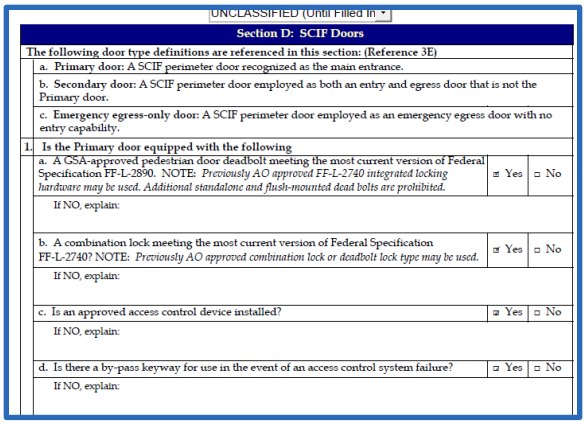
- ○ Sam leaves a description of the ceiling tiles under subsection 4, item b "Describe Perimeter Wall Construction".
- ○ Sam describes the material and thickness of the ceiling under subsection 4, item c, "True ceiling."
- ○ Sam marks the checkbox "Yes" under subsection 4, item d "False ceiling?" and describes the type of ceiling material and distance between the true and false ceiling.
- ○ Sam does not need to provide details about the ceiling tiles on the FFC.

Section D: SAPF Doors

Section D of the FFC focuses on one key penetrable area—doors. In the SAPF Doors section, you describe the doors that are used to access the SAPF and the protections that are in place. This includes the primary doors, secondary doors, criteria for all SAPF doors, and door fabrication.

Primary Doors

Review information on Primary Doors, found in subsection 1.



UNCLASSIFIED (Until Filled In)

Section D: SCIF Doors

The following door type definitions are referenced in this section: (Reference 3E)

a. Primary door: A SCIF perimeter door recognized as the main entrance.

b. Secondary door: A SCIF perimeter door employed as both an entry and egress door that is not the Primary door.

c. Emergency egress-only door: A SCIF perimeter door employed as an emergency egress door with no entry capability.

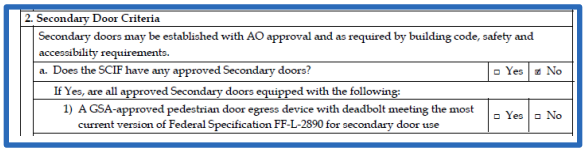
1. Is the Primary door equipped with the following

a. A GSA-approved pedestrian door deadbolt meeting the most current version of Federal Specification FF-L-2890. NOTE: *Previously AO approved FF-L-2740 integrated locking hardware may be used. Additional standalone and flush-mounted dead bolts are prohibited.*	☒ Yes	☐ No
If NO, explain:		
b. A combination lock meeting the most current version of Federal Specification FF-L-2740? NOTE: *Previously AO approved combination lock or deadbolt lock type may be used.*	☒ Yes	☐ No
If NO, explain:		
c. Is an approved access control device installed?	☒ Yes	☐ No
If NO, explain:		
d. Is there a by-pass keyway for use in the event of an access control system failure?	☐ Yes	☐ No
If NO, explain:		

Subsection/Question	Important Information
1. Is the Primary door equipped with the following	In the **Primary Door** subsection include information for the General Services Administration (GSA) approved pedestrian door, deadbolts, hardware, and combination locks.
a. A GSA-approved pedestrian deadbolt meeting the most current version of Federal Specification FF-L-2890. b. A combination lock meeting the most current version of Federal Specification FF-L-2740?	You need to verify that model FF-L-2890 for deadbolts and hardware, and model FF-L-2740 for combination locks are installed.
c. Is an approved access control device installed? d. Is there a by-pass keyway for use in the event of an access control system failure?	You also include information on access control devices and by-pass keys.

Secondary Doors

Review subsection 2: Secondary Doors.



2. Secondary Door Criteria

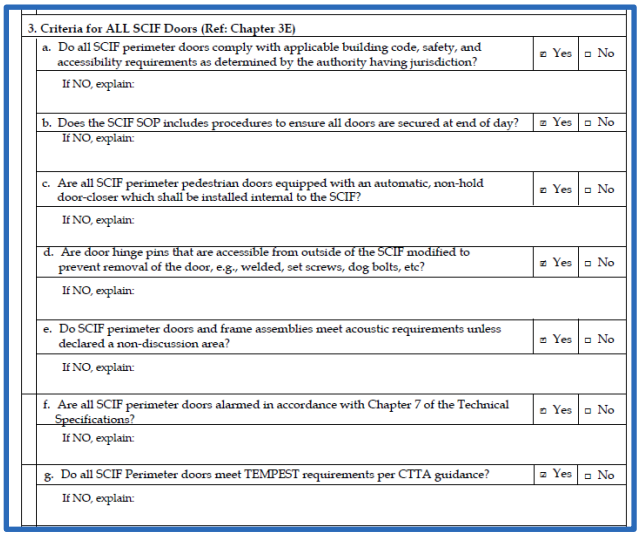
Secondary doors may be established with AO approval and as required by building code, safety and accessibility requirements.

a. Does the SCIF have any approved Secondary doors?	☐ Yes	☒ No
If Yes, are all approved Secondary doors equipped with the following:		
1) A GSA-approved pedestrian door egress device with deadbolt meeting the most current version of Federal Specification FF-L-2890 for secondary door use	☐ Yes	☐ No

Subsection	Important Information
2. Secondary Door Criteria	Similarly, in the **Secondary Doors** subsection, you include information on GSA-approved hardware, emergency egress, and alarms.

All SAPF Doors

Review the Criteria for ALL SAPF Doors in subsection 3.

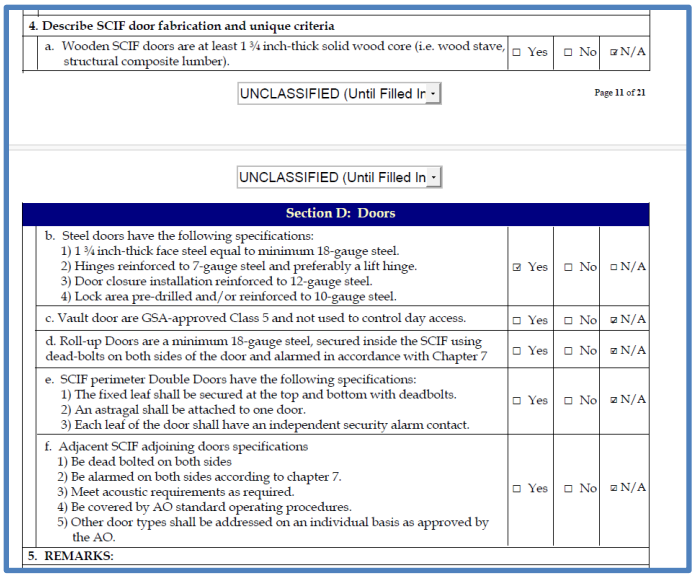


3. Criteria for ALL SCIF Doors (Ref: Chapter 3E)		
a. Do all SCIF perimeter doors comply with applicable building code, safety, and accessibility requirements as determined by the authority having jurisdiction?	☒ Yes	☐ No
If NO, explain:		
b. Does the SCIF SOP includes procedures to ensure all doors are secured at end of day?	☒ Yes	☐ No
If NO, explain:		
c. Are all SCIF perimeter pedestrian doors equipped with an automatic, non-hold door-closer which shall be installed internal to the SCIF?	☒ Yes	☐ No
If NO, explain:		
d. Are door hinge pins that are accessible from outside of the SCIF modified to prevent removal of the door, e.g., welded, set screws, dog bolts, etc?	☒ Yes	☐ No
If NO, explain:		
e. Do SCIF perimeter doors and frame assemblies meet acoustic requirements unless declared a non-discussion area?	☒ Yes	☐ No
If NO, explain:		
f. Are all SCIF perimeter doors alarmed in accordance with Chapter 7 of the Technical Specifications?	☒ Yes	☐ No
If NO, explain:		
g. Do all SCIF Perimeter doors meet TEMPEST requirements per CTTA guidance?	☒ Yes	☐ No
If NO, explain:		

Subsection	Important Information
3. Criteria for ALL SCIF Doors (Ref: Chapter 3E)	In the **Criteria for ALL SAPF Doors** subsection, you provide details of all SAPF door features. These features follow criteria that must be met or have an SAPF-AO awareness or approval for not meeting.
	Criteria incudes meeting codes for safety and accessibility, following standard operating procedures (SOP), having an automatic non-hold door closer internal to the SAPF, having secured hinge pins, meeting acoustic requirements for door frames, having alarms, and meeting TEMPEST requirements.

Door Fabrication

Review subsection 4: Door Fabrication.



4. Describe SCIF door fabrication and unique criteria			
a. Wooden SCIF doors are at least 1 ¾ inch-thick solid wood core (i.e. wood stave, structural composite lumber).	☐ Yes	☐ No	☑ N/A

UNCLASSIFIED (Until Filled In

Page 11 of 21

UNCLASSIFIED (Until Filled In

Section D: Doors			
b. Steel doors have the following specifications: 1) 1 ¾ inch-thick face steel equal to minimum 18-gauge steel. 2) Hinges reinforced to 7-gauge steel and preferably a lift hinge. 3) Door closure installation reinforced to 12-gauge steel. 4) Lock area pre-drilled and/or reinforced to 10-gauge steel.	☑ Yes	☐ No	☐ N/A
c. Vault door are GSA-approved Class 5 and not used to control day access.	☐ Yes	☐ No	☑ N/A
d. Roll-up Doors are a minimum 18-gauge steel, secured inside the SCIF using dead-bolts on both sides of the door and alarmed in accordance with Chapter 7	☐ Yes	☐ No	☑ N/A
e. SCIF perimeter Double Doors have the following specifications: 1) The fixed leaf shall be secured at the top and bottom with deadbolts. 2) An astragal shall be attached to one door. 3) Each leaf of the door shall have an independent security alarm contact.	☐ Yes	☐ No	☑ N/A
f. Adjacent SCIF adjoining doors specifications 1) Be dead bolted on both sides 2) Be alarmed on both sides according to chapter 7. 3) Meet acoustic requirements as required. 4) Be covered by AO standard operating procedures. 5) Other door types shall be addressed on an individual basis as approved by the AO.	☐ Yes	☐ No	☑ N/A
5. REMARKS:			

Subsection	Important Information
4. Describe SCIF door fabrication and unique criteria.	In the **Describe SAPF Door Fabrication and Unique Criteria** subsection, you ensure the fabrication or construction of the door meets requirements, including material-specific specs and type-specific specs.

Knowledge Check

Now try this one.

Cameron is evaluating a SAPF and is completing Section D (SAPF Doors) of the FFC. He is considering the fabrication requirements for steel and wood doors. What is the required thickness of steel and wood doors in a SAPF?

Select the best response. Check your answers in the Answer Key at the end of this Student Guide.

- ○ 6 inches thick
- ○ 1 ¾ inches thick
- ○ 2 ¾ inches thick
- ○ 2 inches thick

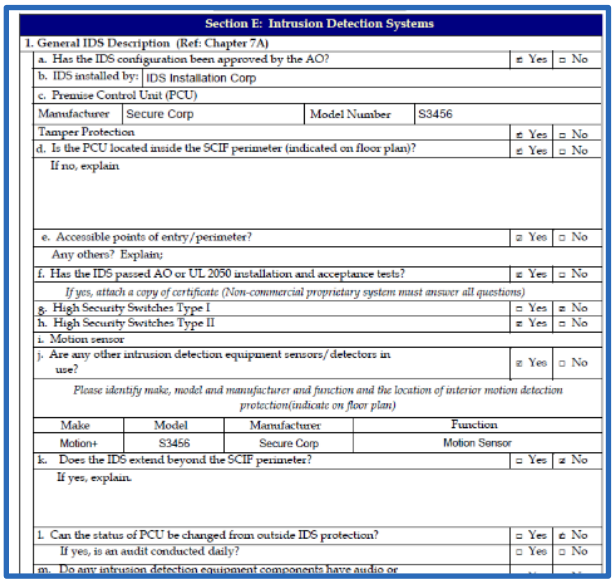
Section E: Intrusion Detection System

Section E focuses on the Intrusion Detection System, or IDS. The IDS is a security system that detects and responds to physical threats to a SAPF.

The IDS deters; detects; and documents intrusion with the use of sensors, control panels, and alarms. In the IDS section, you provide a general IDS description and specific details on emergency power, the alarm monitoring station, remote capabilities, automatic features, dial-out capabilities of the facility, and information about the IDS response personnel.

General IDS Description

Review information about the General IDS Description required in subsection 1.



Section E: Intrusion Detection Systems

1. General IDS Description (Ref: Chapter 7A)

a. Has the IDS configuration been approved by the AO?		☒ Yes	☐ No
b. IDS installed by:	IDS Installation Corp		
c. Premise Control Unit (PCU)			
Manufacturer: Secure Corp	Model Number: S3456		
Tamper Protection		☒ Yes	☐ No
d. Is the PCU located inside the SCIF perimeter (indicated on floor plan)?		☒ Yes	☐ No
If no, explain			
e. Accessible points of entry/perimeter?		☒ Yes	☐ No
Any others? Explain:			
f. Has the IDS passed AO or UL 2050 installation and acceptance tests?		☒ Yes	☐ No
If yes, attach a copy of certificate (Non-commercial proprietary system must answer all questions)			
g. High Security Switches Type I		☐ Yes	☒ No
h. High Security Switches Type II		☒ Yes	☐ No
i. Motion sensor			
j. Are any other intrusion detection equipment sensors/detectors in use?		☒ Yes	☐ No

Please identify make, model and manufacturer and function and the location of interior motion detection protection(indicate on floor plan)

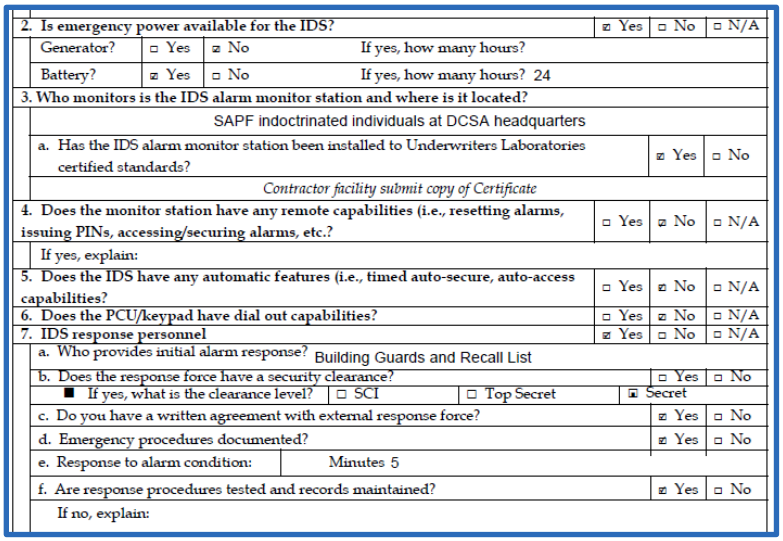
Make	Model	Manufacturer	Function
Motion+	S3456	Secure Corp	Motion Sensor

k. Does the IDS extend beyond the SCIF perimeter?	☐ Yes	☒ No
If yes, explain.		
l. Can the status of PCU be changed from outside IDS protection?	☐ Yes	☒ No
If yes, is an audit conducted daily?	☐ Yes	☐ No
m. Do any intrusion detection equipment components have audio or		

Subsection/Question	Important Information
1. General IDS Description (Ref: Chapter 7A)	In the **General IDS Description** subsection, you provide details about the installation, types of sensors and mounts, locations, range, and use of network connections.
i. Motion sensor j. Are any other intrusion detection equipment sensors/detectors in use?	Typical sensors include UL 639 Sensors and UL 634 High Security Switches (HSS).

Detailed IDS Description

Review information required to provide a Detailed IDS Description in subsections 2 through 7.



2. Is emergency power available for the IDS?			☒ Yes	☐ No	☐ N/A
Generator?	☐ Yes	☒ No	If yes, how many hours?		
Battery?	☒ Yes	☐ No	If yes, how many hours? 24		
3. Who monitors is the IDS alarm monitor station and where is it located?					
SAPF indoctrinated individuals at DCSA headquarters					
a. Has the IDS alarm monitor station been installed to Underwriters Laboratories certified standards?				☒ Yes	☐ No
Contractor facility submit copy of Certificate					
4. Does the monitor station have any remote capabilities (i.e., resetting alarms, issuing PINs, accessing/securing alarms, etc.?				☐ Yes	☒ No ☐ N/A
If yes, explain:					
5. Does the IDS have any automatic features (i.e., timed auto-secure, auto-access capabilities?				☐ Yes	☒ No ☐ N/A
6. Does the PCU/keypad have dial out capabilities?				☐ Yes	☒ No ☐ N/A
7. IDS response personnel				☒ Yes	☐ No ☐ N/A
a. Who provides initial alarm response? Building Guards and Recall List					
b. Does the response force have a security clearance?				☐ Yes	☐ No
■ If yes, what is the clearance level?	☐ SCI	☐ Top Secret	☒ Secret		
c. Do you have a written agreement with external response force?				☒ Yes	☐ No
d. Emergency procedures documented?				☒ Yes	☐ No
e. Response to alarm condition:	Minutes 5				
f. Are response procedures tested and records maintained?				☒ Yes	☐ No
If no, explain:					

Subsection	Important Information
2. Is emergency power available for the IDS? 3. Who monitors the IDS alarm monitor station and where is it located? 4. Does the monitor station have any remote capabilities?	You state if emergency power is available to the IDS, who monitors the alarm station, and any remote capabilities it has.
5. Does the IDS have any automatic features? 6. Does the PCU/keypad have dial out capabilities?	You also note if the IDS has automatic features and if the Premise Control Unit (PCU) or keypad has any dial-out capabilities.
7. IDS response personnel	You provide details about the personnel responsible for providing initial alarm responses, their security clearance level, and the expected response times.

Section F: Telecommunication Systems and Equipment Baseline

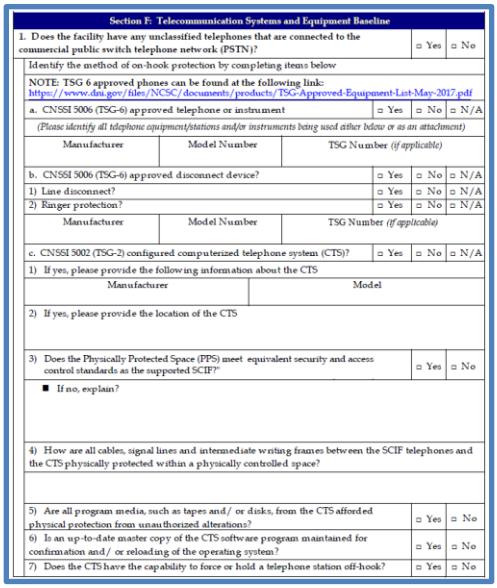
Section F outlines the security requirements for telecommunication systems and equipment baselines. The information you provide in Section F ensures protection of information and details the configuration of unclassified telecommunications systems, device features and software, access control, and control of the cable infrastructure.

Communication equipment in Section F includes telephones; voicemail or telephone answering devices; Multi-function Office Machines (M-FOMs); Video Teleconference devices (VTC); other television receivers; and countermeasure systems.

Remember to use the most up-to-date Telephone System Group (TSG) approved equipment list.

Unclassified Telephones

Review subsection 1: Unclassified Telephones.



Section F: Telecommunication Systems and Equipment Baseline

1. Does the facility have any unclassified telephones that are connected to the commercial public switch telephone network (PSTN)? ☐ Yes ☐ No

Identify the method of on-hook protection by completing items below

NOTE: TSG 6 approved phones can be found at the following link: https://www.dni.gov/files/NCSC/documents/products/TSG-Approved-Equipment-List-May-2017.pdf

a. CNSSI 5006 (TSG-6) approved telephone or instrument ☐ Yes ☐ No ☐ N/A

(Please identify all telephone equipment/stations and/or instruments being used either below or as an attachment)

Manufacturer	Model Number	TSG Number *(if applicable)*

b. CNSSI 5006 (TSG-6) approved disconnect device? ☐ Yes ☐ No ☐ N/A

1) Line disconnect? ☐ Yes ☐ No ☐ N/A

2) Ringer protection? ☐ Yes ☐ No ☐ N/A

Manufacturer	Model Number	TSG Number *(if applicable)*

c. CNSSI 5002 (TSG-2) configured computerized telephone system (CTS)? ☐ Yes ☐ No ☐ N/A

1) If yes, please provide the following information about the CTS

Manufacturer	Model

2) If yes, please provide the location of the CTS

3) Does the Physically Protected Space (PPS) meet equivalent security and access control standards as the supported SCIF?* ☐ Yes ☐ No

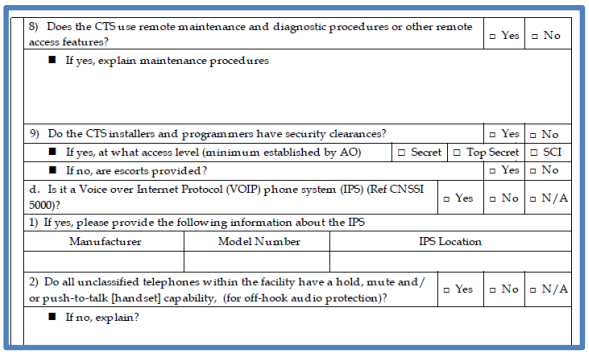
■ If no, explain?

4) How are all cables, signal lines and intermediate writing frames between the SCIF telephones and the CTS physically protected within a physically controlled space?

5) Are all program media, such as tapes and/ or disks, from the CTS afforded physical protection from unauthorized alterations? ☐ Yes ☐ No

6) Is an up-to-date master copy of the CTS software program maintained for confirmation and/ or reloading of the operating system? ☐ Yes ☐ No

7) Does the CTS have the capability to force or hold a telephone station off-hook? ☐ Yes ☐ No



8) Does the CTS use remote maintenance and diagnostic procedures or other remote access features? ☐ Yes ☐ No

■ If yes, explain maintenance procedures

9) Do the CTS installers and programmers have security clearances? ☐ Yes ☐ No

■ If yes, at what access level (minimum established by AO) ☐ Secret ☐ Top Secret ☐ SCI

■ If no, are escorts provided? ☐ Yes ☐ No

d. Is it a Voice over Internet Protocol (VOIP) phone system (IPS) (Ref CNSSI 5000)? ☐ Yes ☐ No ☐ N/A

1) If yes, please provide the following information about the IPS

Manufacturer	Model Number	IPS Location

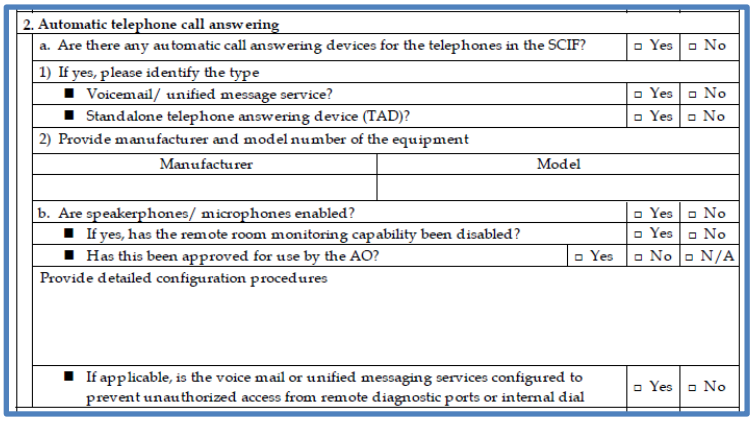
2) Do all unclassified telephones within the facility have a hold, mute and/ or push-to-talk [handset] capability, (for off-hook audio protection)? ☐ Yes ☐ No ☐ N/A

■ If no, explain?

Subsection	Important Information
1. Does the facility have any unclassified telephones that are connected to the commercial public switch telephone network (PSTN)?	In the **Unclassified Telephones** subsection, you provide information about the model number of telephones; memory storage; remote maintenance and diagnostic abilities; telephone lines; and functions like hold, mute, and push to talk.

Automatic Telephone Call Answering

Review the information in subsection 2: Automatic Telephone Call Answering.



2. Automatic telephone call answering

a. Are there any automatic call answering devices for the telephones in the SCIF? ☐ Yes ☐ No

1) If yes, please identify the type

■ Voicemail/ unified message service? ☐ Yes ☐ No

■ Standalone telephone answering device (TAD)? ☐ Yes ☐ No

2) Provide manufacturer and model number of the equipment

Manufacturer	Model

b. Are speakerphones/ microphones enabled? ☐ Yes ☐ No

■ If yes, has the remote room monitoring capability been disabled? ☐ Yes ☐ No

■ Has this been approved for use by the AO? ☐ Yes ☐ No ☐ N/A

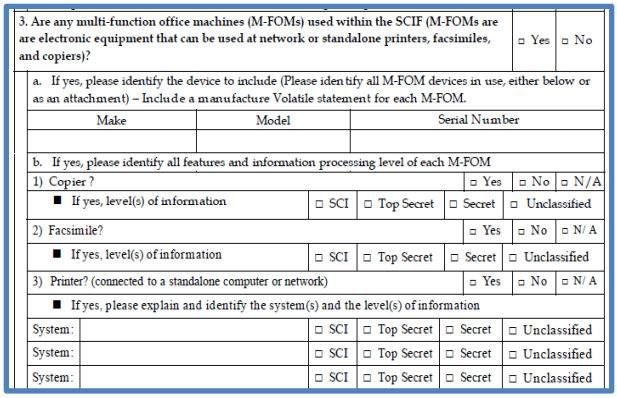
Provide detailed configuration procedures

■ If applicable, is the voice mail or unified messaging services configured to prevent unauthorized access from remote diagnostic ports or internal dial ☐ Yes ☐ No

Subsection	Important Information
2. Automatic telephone call answering	In the **Automatic Telephone Call Answering** subsection you identify existing call answering devices (like voicemail or telephone answering devices) and provide equipment information.

Multi-function Office Machines

Review the requirements of M-FOMs in subsection 3.



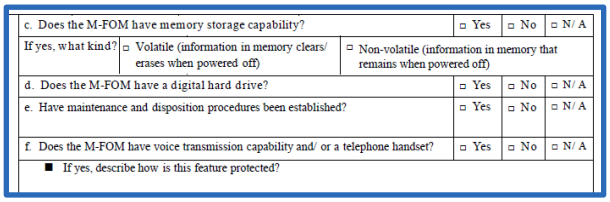
3. Are any multi-function office machines (M-FOMs) used within the SCIF (M-FOMs are are electronic equipment that can be used at network or standalone printers, facsimiles, and copiers)?	□ Yes	□ No

a. If yes, please identify the device to include (Please identify all M-FOM devices in use, either below or as an attachment) – Include a manufacture Volatile statement for each M-FOM.

Make	Model	Serial Number

b. If yes, please identify all features and information processing level of each M-FOM

1) Copier ?				□ Yes □ No	□ N/A
■ If yes, level(s) of information	□ SCI	□ Top Secret	□ Secret	□ Unclassified	
2) Facsimile?				□ Yes □ No	□ N/ A
■ If yes, level(s) of information	□ SCI	□ Top Secret	□ Secret	□ Unclassified	
3) Printer? (connected to a standalone computer or network)				□ Yes □ No	□ N/ A
■ If yes, please explain and identify the system(s) and the level(s) of information					
System:		□ SCI	□ Top Secret	□ Secret	□ Unclassified
System:		□ SCI	□ Top Secret	□ Secret	□ Unclassified
System:		□ SCI	□ Top Secret	□ Secret	□ Unclassified

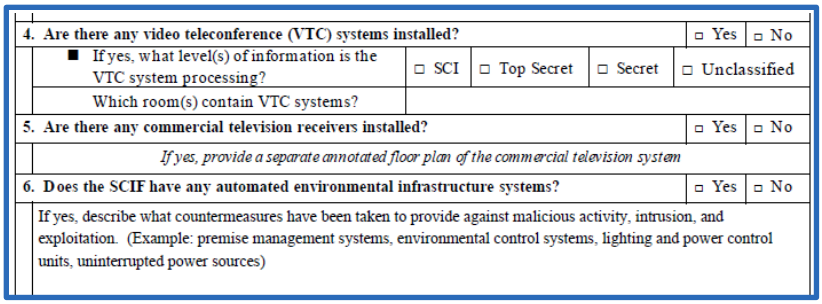


c. Does the M-FOM have memory storage capability?	□ Yes	□ No	□ N/ A
If yes, what kind? □ Volatile (information in memory clears/ erases when powered off) □ Non-volatile (information in memory that remains when powered off)			
d. Does the M-FOM have a digital hard drive?	□ Yes	□ No	□ N/ A
e. Have maintenance and disposition procedures been established?	□ Yes	□ No	□ N/ A
f. Does the M-FOM have voice transmission capability and/ or a telephone handset?	□ Yes	□ No	□ N/ A
■ If yes, describe how is this feature protected?			

Subsection	Important Information
3	M-FOMs are machines that combine multiple functions on one device, such as copiers, printers, scanners, and facsimiles.
3. Are any multi-function office machines (M-FOMs) used within the SCIF?	In the **M-FOM** subsection, you provide information on the types and models of equipment present in the facility; the equipment's memory storage; hard drives; and transmission capabilities like Bluetooth, wireless, or non-approved network.

VTC, Receivers, and Countermeasure Systems

Review subsections 4, 5, and 6: VTC, Receivers, and Countermeasure Systems.



4. Are there any video teleconference (VTC) systems installed?				☐ Yes	☐ No
■ If yes, what level(s) of information is the VTC system processing?	☐ SCI	☐ Top Secret	☐ Secret	☐ Unclassified	
Which room(s) contain VTC systems?					
5. Are there any commercial television receivers installed?				☐ Yes	☐ No
If yes, provide a separate annotated floor plan of the commercial television system					
6. Does the SCIF have any automated environmental infrastructure systems?				☐ Yes	☐ No
If yes, describe what countermeasures have been taken to provide against malicious activity, intrusion, and exploitation. (Example: premise management systems, environmental control systems, lighting and power control units, uninterrupted power sources)					

Subsection	Important Information
4. Are there any video teleconference (VTC) systems installed?	The **VTC** subsection requires you to detail what information is being relayed outside the SAPF via VTC and how classified information is being protected.
5. Are there any commercial television receivers installed?	In the **Commercial Television Receivers** subsection, you ensure data is only being received into the SAPF via commercial television receivers and not going out through Bluetooth or other wireless means.
6. Does the SCIF have any automated environmental infrastructure systems?	Make sure you illustrate what countermeasures are in place to avoid malicious activity, intrusion, and exploitation.

Section G: Acoustical Protection

Acoustical protection is a vital component of securing SAPFs.

The SAPF-AO tests to determine if the SAPF meets acoustical protection standards and is pivotal to completing Section G.

Acoustic Security Standards

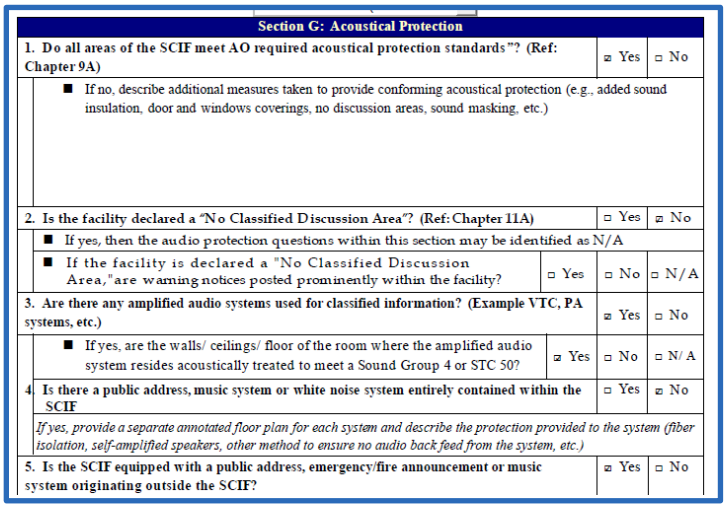
The ability of an SAPF structure to retain sound within the perimeter is rated using a descriptive value called the Sound Transmission Class (STC).

To satisfy the normal security standards of SAPFs, two transmission attenuation groups were established.

- Sound Group 3 is a rating of STC 45 or better and includes loud speech from within the SAPF that can be faintly heard but not understood outside the SAPF. In this group, normal speech is unintelligible with the unaided human ear.
- Sound Group 4 is a rating of STC 50 or better and includes very loud sounds within the SAPF such as loud singing, brass music, or a radio at full volume that can be heard with the human ear faintly or not at all outside of the SAPF.

Subsection Information

Now, review information about Acoustical Protections in subsections 1 through 5.



Section G: Acoustical Protection			
1. Do all areas of the SCIF meet AO required acoustical protection standards"? (Ref: Chapter 9A)		☒ Yes	☐ No
■ If no, describe additional measures taken to provide conforming acoustical protection (e.g., added sound insulation, door and windows coverings, no discussion areas, sound masking, etc.)			
2. Is the facility declared a "No Classified Discussion Area"? (Ref: Chapter 11A)		☐ Yes	☒ No
■ If yes, then the audio protection questions within this section may be identified as N/A			
■ If the facility is declared a "No Classified Discussion Area," are warning notices posted prominently within the facility?	☐ Yes	☐ No	☐ N/A
3. Are there any amplified audio systems used for classified information? (Example VTC, PA systems, etc.)		☒ Yes	☐ No
■ If yes, are the walls/ ceilings/ floor of the room where the amplified audio system resides acoustically treated to meet a Sound Group 4 or STC 50?	☒ Yes	☐ No	☐ N/A
4. Is there a public address, music system or white noise system entirely contained within the SCIF		☐ Yes	☒ No
If yes, provide a separate annotated floor plan for each system and describe the protection provided to the system (fiber isolation, self-amplified speakers, other method to ensure no audio back feed from the system, etc.)			
5. Is the SCIF equipped with a public address, emergency/fire announcement or music system originating outside the SCIF?		☒ Yes	☐ No

Subsection	Important Information and Reminders
1. Do all areas of the SCIF meet AO required acoustical protection standards?	State if all areas of the SAPF meet AO-required acoustical protection standards.
2. Is the facility declared a "No Classified Discussion Area"? (Ref: Chapter 11A)	Specify if the facility is declared a "No Classified Discussion Area."
3. Are there any amplified audio systems used for classified information?	State the existence of and provide information on any systems that affect acoustical security, including amplified audio systems used for classified information.
4. Is there a public address, music system or white noise system entirely contained within the SCIF 5. Is the SCIF equipped with a public address, emergency/fire announcement or music system originating outside the SCIF?	Include any outside origin systems like PA, emergency, fire, or music system originating outside the facility.

Section H: Classified Destruction Methods

Section H requires you to include information about the destruction methods for classified/sensitive material used within the SAPF, including listing equipment used.

The PSO is responsible for authorizing the destruction of SAP material and overseeing the destruction of non-standard SAP material through approved equipment.

You can find National Security Agency/Central Security Service (NSA/CSS) approved equipment and their respective destruction procedures on NSA/CSS Evaluated Products Lists (EPLs).

For guidance on the destruction of SAP materials, refer to DODM 5205.07.

Section I: Information Systems/TEMPEST/Technical Security

Section I of the FFC requires information about the TEMPEST security measures and other technical or information security details of the SAPF.

You must consider TEMPEST security measures if electronic processing will occur in the any of the following types of SAP facilities or areas:

- SAPF
- Temporary SAPF (T-SAPF)
- SAP Compartmented Areas (SAPCA)
- SAP Working Areas (SAPWA)
- SAP Temporary Secure Working Areas (SAPTSWA)

Note the SAPF-AO will submit plans to a CTTA and complete the required TEMPEST checklist.

Conclusion

Congratulations. You completed the Fixed Facility Checklist Short. You should now be able to indicate the appropriate actions for completing the FFC for a SAPF. Remember, your ability to perform the actions required of the FFC is vital in maintaining the security of SAPFs.

Working with other designated security professionals and reviewing relevant policies will ensure you are able to complete the FFC with fidelity.

As you navigate the FFC, keep in mind that there are additional types of forms and plans available, depending on the type of facility and classification. Additional forms include TEMPEST Checklist; Compartmented Area Checklist; Shipboard Checklist; Submarine Checklist; Aircraft/Unmanned Aerial Vehicle (UAV) Checklist; and Co-Use Request and Memorandum of Agreement (MOA).

Refer to the Resources provided in this Short to access policies including NCSC SCIF Specifications, DODM 5205.07, as well as the NSA/CSS EPLs and SAPF Wall Types Job Aid.

Appendix A: Answer Key

Knowledge Check 1

Sam is evaluating a SAPF and is completing Section C (SAPF Security) of the FFC. Sam is inspecting the construction of the ceiling and notices the use of ceiling tiles in the SAPF. Which of the following statements correctly indicates how Sam should note the use of ceiling tiles on the FFC?

Select the best response. Check your answer in the Answer Key at the end of this Student Guide.

- ○ Sam leaves a description of the ceiling tiles under subsection 4, item b "Describe Perimeter Wall Construction".
- ○ Sam describes the material and thickness of the ceiling under subsection 4, item c, "True ceiling."
- ⊙ Sam marks the checkbox "Yes" under subsection 4, item d "False ceiling?" and describes the type of ceiling material and distance between the true and false ceiling. (correct response)
- ○ Sam does not need to provide details about the ceiling tiles on the FFC.

***Feedback**: Ceiling tiles are considered false ceilings. Sam will need to check "Yes" under subsection 4, item d and describe the details of the false ceiling.*

Knowledge Check 2

Cameron is evaluating a SAPF and is completing Section D (SAPF Doors) of the FFC. He is considering the fabrication requirements for steel and wood doors. What is the required thickness of steel and wood doors in a SAPF?

Select the best response. Check your answers in the Answer Key at the end of this Student Guide.

- ○ 6 inches thick
- ⊙ 1 ¾ inches thick (correct response)
- ○ 2 ¾ inches thick
- ○ 2 inches thick

***Feedback**: Cameron must ensure the wood and steel doors in the SAPF are 1 ¾ inches thick.*