SCIF Fixed Facility Checklist V1.5

FFC Date:

CLASSIFY ACCORDING TO CLASSIFICATION AUTHORITY

CHECK Applicable blocks		
☐ Domestic	☐ Overseas Not COM	☐ Overseas COM
☐ Pre-construction, Complete Sections as Required by A/O	☐ Final FFC Accreditation	☐ Update/Page Change

Checklist Contents

List of Attachments

Section A: General Information

1. SCIF Data

Accrediting Agency	
Organization/Company Name	
SCIF Identification Number *(if applicable)*	
Organization subordinate to *(if applicable)*	
Contract Number & Expiration Date *(if applicable)*	
Concept approval Date/by *(if applicable)*	
Accrediting Office/Accrediting Individual's Name	/

Defense Special Security Communication System (DSSCS) Information *(if applicable)*

DSSCS Message Address	
DSSCS INFO Address	
If no DSSCS Message Address, please provide passing instructions	

2. SCIF Location

Street Address		
Lat/Long (*If No Street*)	/	
Building Name		
Floor(s)	Suite(s)	Room(s) #
City	Base/Post	
State/Country /		Zip Code

3. Mailing Address (if different from SCIF location)

Street or Post Office Box		
City	State	Zip Code

4. Responsible Security Personnel

	PRIMARY	ALTERNATE
Name		
Commercial Phone		
DSN Phone		
Secure Phone Type		
Cell		
Secure Fax		
Class Email		
Unclass Email		
Other Email		

Command or Regional Special Security Office/Name (SSO) *(if applicable)*

Name	
Commercial Phone	
Other Phone	

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:

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:	Days Per Week:

g. Total square footage that the SCIF occupies:

h. Does the facility have any approved waivers?	☐ Yes	☐ No

Provide attachment if required by AO

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:	On		
2) Were deficiencies corrected?	☐ Yes	☐ No	☐ N/A

3) If NO, explain:

b. Last AO compliance periodic inspection/review:	On
AO Office Name	AO Individual's Name
c. Last self Inspection completed by:	On

Were deficiencies corrected?	☐ Yes	☐ No	☐ N/A

If NO, explain:

8. REMARKS:

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		
2) Building Lighting		
h. Is there external CCTV coverage?	☐ Yes	☐ No
If so, describe the CCTV system. *(include monitor/coverage locations on map)*		
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?		
4) Any SCIF duties?	☐ Yes	☐ No
If yes, describe duties:		

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	
c. Windows	
d. Doors	

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

4. Remarks (Describe any additional security measures not addressed in this section)

What external security attributes and/or features should the AO consider before determining whether or not this facility has Security In-Depth? Please identify/explain all factors:

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:	Model:		
(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

2. Does the SCIF have windows? (Ref: Chapter 3F) ☐ Yes ☐ No ☐ N/A

a. Are they acoustically protected?		☐ Yes	☐ No ☐ N/A
If Yes, how: If No, explain:			
b. Are they secured against forced entry?		☐ Yes	☐ No ☐ N/A
If Yes, how: If No, explain:			
c. Do they have RF protection?		☐ Yes	☐ No ☐ N/A
If Yes, describe:			

2. SCIF windows (continued) (Ref: Chapter 3F)

d. Are they protected against visual surveillance?	☐ Yes	☐ No	☐ N/A
If Yes, how: If No, explain:			

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:		

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:		
c. True ceiling		
Describe material and 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:		
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?		

4. REMARKS:

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:		

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
If NO, explain:		
2) Approved access control hardware which must be deactivated when the SCIF is not occupied, or as determined by the AO.	☐ Yes	☐ No
If NO, explain:		
b. Does the SCIF have any Emergency Egress-only doors?	☐ Yes	☐ No
If Yes, do all approved Emergency Egress-only doors meet the following:		
1) Are they installed as required by building code, safety and accessibility requirements?	☐ Yes	☐ No
If NO, explain:		

Section D: SCIF Doors

2) Are they equipped with GSA-approved pedestrian door emergency egress device with deadbolt configuration meeting the most current version of Federal Specification FFL-2890 for exit only door use or an AO approved alternate device with similar functionality ?	□ Yes	□ No
If NO, explain:		
3) Are they alarmed 24/7 and have a local audible annunciator that must be activated if the door is opened?	□ Yes	□ No
If NO, explain:		

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:		

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

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:

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:		
c. Premise Control Unit (PCU)		
Manufacturer	Model Number	
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

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 video capabilities?	□ Yes	□ No
If yes, explain.		
n. PCU administrator SCI indoctrinated?	□ Yes	□ No
o. Is external Transmission Line Security used?	□ Yes	□ No
If yes, explain.		
p. What is the method of line security? National Institute of Standards and Technology (NIST) FIPS AES encryption?	□ Yes	□ No

1) If yes, has the encryption been certified by NIST or another independent testing laboratory?	□ Yes	□ No	
2) If not NIST standard, is there an alternate?	□ Yes	□ No	
If yes, explain.			
3) Does the alternate line utilize any cellular or other Radio Frequency (RF) capability?	□ Yes	□ No	
Manufacturer	Model Number		
q. Does any part of the IDS use local or wide area network (LAN/WAN)?	□ Yes	□ No	□ N/A
1) Is the host computer dedicated solely for security purposes?	□ Yes	□ No	□ N/A
2) Is the host computer secured within an alarmed area at the physically or higher level protected spaces or higher level?	□ Yes	□ No	□ N/A
3) Is the host computer protected through firewalls or similar devices?	□ Yes	□ No	□ N/A
4) Is the password for the host computer unique for each user and at least 8-characters long consisting of alpha, numeric, and special characters?	□ Yes	□ No	□ N/A
5) Is the password changed semi-annually?	□ Yes	□ No	□ N/A
6) Are remote security terminals protected the same as the host computer?	□ Yes	□ No	□ N/A
If no, explain:			

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?		

3. Who monitors is the IDS alarm monitor station and where is it located?

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?			
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		
f. Are response procedures tested and records maintained?		□ Yes	□ No
If no, explain:			

g. Has a catastrophic failure plan been approved by the AO?	□ Yes	□ No

■ If no, explain:

10. REMARKS:

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?			
3) Is access to the facility housing the IPS physically controlled?		☐ Yes	☐ No
■ If yes, what is the clearance level (if any) of facility or area where the switch is located and how is the area controlled?	☐ Secret ☐ Top Secret ☐ SCI		
■ If no facility clearance level how is the facility or area where the IPS is physically located controlled			
4) Are all cables, signal lines and intermediate wiring frames between the SCIF telephones and the IPS physically protected or contained within a physically controlled space?		☐ Yes	☐ No
■ If no, explain?			
5) Are all program media, such as tapes and/ or disks, from the IPS afforded physical protection from unauthorized alterations?		☐ Yes	☐ No
6) Is an up-to-date master copy of the IPS software program maintained for confirmation and/ or reloading of the operating system?		☐ Yes	☐ No
7) Does the IPS have the capability to force or hold a telephone station off-hook?		☐ Yes	☐ No

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

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

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?			

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)				

7. REMARKS:

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

6. REMAKS:

Section H: Classified Destruction Methods

1. Destruction methods? (Ref: Chapter 12M)

a. Describe the method and equipment used for destruction of classified/ sensitive material (if more than one method or device, use Remarks to describe). List all manufacturer and models

Method	Device Manufacturer	Model

b. Is a secondary method of destruction available?	☐ Yes	☐ No	
c. Describe the location of destruction site(s) in relation to the secure facility			
d. Describe method or procedure used for handling non-soluble classified/ sensitive material at this facility			
e. Do you have a written Emergency Action Plan (EAP) approved by AO (if required)?	☐ Yes	☐ No	☐ N/ A

2. REMARKS:

Section I: INFOSEC/TEMPEST/Technical Security

1.	**Does the facility electronically process classified information? (Ref: Chapter 13)**	☐ Yes	☐ No
	■ If yes, complete TEMPEST CHECKLIST FOR SCIF Form		