

SCIF Fixed Facility Checklist

Organization Name:

FFC Date:

CLASSIFY ACCORDING TO CLASSIFICATION AUTHORITY

CHECK Applicable blocks		
<input type="checkbox"/> Domestic	<input type="checkbox"/> Overseas Not COM	<input type="checkbox"/> Overseas COM
<input type="checkbox"/> Pre-construction, Complete Sections as Required by A/O	<input type="checkbox"/> Final FFC Accreditation	<input type="checkbox"/> Update/Page Change

Checklist Contents

Section A: General Information

Section B: Security-in-Depth

Section C: SCIF Security

Section D: Doors

Section E: Intrusion Detection Systems (IDS)

Section F: Telecommunication Systems and Equipment Baseline

Section G: Acoustical Protection

Section H: Classified Destruction Methods

Section I: Information Systems/TEMPEST/Technical Security

List of Attachments

-- TEMPEST Checklist

-- Diagrams and Other Attachments as Required

Section A: General Information

1. SCIF Data

Organization/Company Name		
SCIF Identification Number <i>(if applicable)</i>		
Organization subordinate to <i>(if applicable)</i>		
Contract Number & Expiration Date <i>(if applicable)</i>		
Concept approval Date/by <i>(if applicable)</i>		
Cognizant Security Authority (CSA)	CSA	
Defense Special Security Communication System Information <i>(if applicable)</i>		
DSSCS Message Address		
DSSCS INFO Address		
If no DSSCS Message Address, please provide passing instructions		

2. SCIF Location

Street Address		Building Name	
Floor(s)	Suite(s)	Room(s) #	
City		Base/Post	
State/Country ST /		Zip Code	

3. Mailing Address (if different from SCIF location)

Street or Post Office Box		
City	State ST	Zip Code

4. Responsible Security Personnel

	PRIMARY	ALTERNATE
Name		
Commercial Phone		
DSN Phone		
Secure Phone		
STE Other Phone		
Home		
Secure Fax		
Command or Regional Special Security Office/Name (SSO) <i>(if applicable)</i>		
Commercial Phone		
Other Phone		

5. E-Mail Address of Responsible Security Personnel			
Classified	Network/System Name & Level		
Unclassified	Network/System Name		
Other	Network/System Name		
6. Accreditation Data (Ref Chapter: 12E)			
a. Category/Compartments of SCI Requested:			
1) Indicate storage requirement:			
<input type="checkbox"/> Open	<input type="checkbox"/> Closed	<input type="checkbox"/> Continuous Operation	<input type="checkbox"/> None
2) Indicate the facility type			
<input type="checkbox"/> Permanent	<input type="checkbox"/> Temporary	<input type="checkbox"/> Secure Working Area	<input type="checkbox"/> TSWA
3) Co-Use Agreements			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, provide sponsor:			
b. SAP(s) co-located within SCIF			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, identify SAP Classification level (check all that apply)			
<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Confidential
c. SCIF Duty Hours	Hours to Hours:	Days Per Week:	
d. Total square footage that the SCIF occupies:			
e. Has or will CSA requested any waivers?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
<i>If yes, attach a copy of approved waiver</i>			
7. Construction/Modification (Ref: Chapter 3B)			
a. Is construction or modification complete?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If no, enter the expected date of completion:			
b. Was all construction completed in accordance with the CSP?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If NO, explain:			
8. Inspections (Ref: Chapter 12G) (ALL INSPECTION REPORTS MUST BE ATTACHED)			
a. Has a TSCM Inspection been performed?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, provide the following:			
b. TSCM Service completed by:			On
Were deficiencies corrected?			<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A
If NO, explain:			

c. Last physical security inspection by:	On		
Were deficiencies corrected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
If NO, explain:			
d. Last Staff Assistance Visit by:	On		

9. REMARKS:

--	--	--	--

Section B: Security-in-Depth

1. Describe building exterior Security (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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Is the SCIF located in an entire Building	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Is the SCIF located on a single floor of Building	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Is the SCIF located in a secluded area of Building	<input type="checkbox"/> Yes	<input type="checkbox"/> No
e. Is the SCIF located on a fenced compound with access controlled vehicle gate and/or pedestrian gate?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
f. Fence Type		
1) Height:		
2) Does it surround the compound?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
3) How is it controlled?		
4) How many gates?		
5) Hours of usage?		
6) How are they controlled when not in use?		
Is the Fence Alarmed?	<input type="checkbox"/> Yes	<input type="checkbox"/> 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If so, describe the CCTV system. <i>(include monitor locations on map)</i>		
i. Exterior Guards	<input type="checkbox"/> Yes	<input type="checkbox"/> No
1) What kind of patrols are they?	<input type="checkbox"/> Static	<input type="checkbox"/> Roving
2) Clearance level of guards <i>(if applicable)</i>	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret <input type="checkbox"/> Secret
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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, is SCIF controlled by bldg owners?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If controlled by SCIF owners, is alarm activation reported to SCIF owners by agreement?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Construction Type		
c. Windows		
d. Doors		
e. Describe Building Access Control: Continuous?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, during what hours?		
f. Clearance level of guards <i>(if applicable)</i>	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret
1) Any SCIF duties?	<input type="checkbox"/> Yes	<input type="checkbox"/> 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, describe adjacent areas and types of alarm systems		
b. Controlled by SCIF Owner?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If controlled by Bldg owner, alarm activation reported to SCIF owner by agreement?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

4. Security In-Depth

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:

Remarks:

--

Section C: SCIF Security

1. How is access to the SCIF controlled (Ref: Chapter 8)

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

2. Does the SCIF have windows? (Ref: Chapter 3F)

a. Are they acoustically protected?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
If Yes, explain:			
b. Are they secured against forced entry?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
If Yes, explain:			
c. Are they protected against visual surveillance?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/A
If Yes, explain:			

3. Do ventilation ducts penetrate the SCIF perimeter? (Ref: Chapter 3G)

Yes No

<i>(Indicate all duct penetrations and their size on a separate floor plan as an attachment)</i>			
a. Any ducts over 96 square inches that penetrate perimeter walls?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
If yes, how are they protected?	<input type="checkbox"/> IDS (Describe in Section E)	<input type="checkbox"/> Bars/Grills/Metal / Baffles	
If Other, Describe Protection:			
b. Inspection ports?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
■ If yes, are they within the SCIF?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
■ If no, are they secured?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
If No, explain:			
c. Do all ventilation ducts penetrating the perimeter meet acoustical requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<i>(NOTE: All ducts and vents, regardless of size may require acoustical protection)</i>			
■ If yes, how are they protected?	<input type="checkbox"/> Metal Baffles	<input type="checkbox"/> Noise Generator	<input type="checkbox"/> Z-Duct
If Other, Describe Protection:			

3. Construction (Ref: Chapter 3B)

a. Describe Perimeter Wall Construction:		
b. True ceiling (material and thickness)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If Yes, What is the material and thickness:		
c. False ceiling?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
1) If yes, what is the type of ceiling material?		
2) What is the distance between false and true ceiling?		

CLASSIFICATION

d. True floor (material and thickness)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If Yes, What is the material and thickness:		
e. False floor?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
1) If yes, what is the type of false flooring?		
2) What is the distance between false and true floor?		

4. REMARKS:

Section D: Doors

1. Describe SCIF primary entrance door construction (Ref: Chapter 3E)

(Indicate door locations and types floor plan as an attachment)

a. Does the door and doorframe meet sound attenuation requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, have acoustical countermeasures been employed?		
b. Describe SCIF perimeter doors to include thickness and type of door.		
c. Is an automatic door closer installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If NO, explain:		
d. Is a door sweep/thresholds installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If NO, explain:		
e. Is an acoustical/astragal strip installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If NO, explain:		

2. Describe number and type of doors used for SCIF emergency exits and other perimeter doors including day access

a. Do the doors and doorframes meet sound attenuation requirements?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, have acoustical countermeasures been employed?		
b. Has exterior hardware been removed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Has local enunciator been installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Describe how the door hinges exterior to the SCIF are secured against removal (if in an uncontrolled area).		

CLASSIFICATION

3. Locking Devices

a. Is the primary entrance door equipped with a GSA-approved pedestrian door deadbolt meeting Federal Specification FF-L-2890 including lock meeting FF-L-2740A	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. List combination lock manufacturer, model number and group rating		
Manufacturer:		
Model Number:		
Group Rating:		
c. Does the entrance door stand open into an uncontrolled area?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, please describe tamper protection.		
d. Emergency exits and other perimeter doors: Describe (locks, metal strip/bar, deadbolts, local annunciation, and panic hardware).		
e. Where is the lock combination(s) filed? (Please identify the SCIF AO and SCIF ID#)		

4. REMARKS:

Section E: Intrusion Detection Systems

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

a. Has the IDS configuration been approved by the AO?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Identity of IDS installer:		
IDS monitoring firm:		
c. Premise Control Unit (PCU)		
Manufacturer		Model Number
Tamper Protection	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Is the PCU located inside the SCIF perimeter (indicated on floor plan)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, please explain		

CLASSIFICATION

e. Location of interior motion detection protection			
Accessible points of entry/perimeter?			<input type="checkbox"/> Yes <input type="checkbox"/> No
Any others? Explain;			
f. Has the IDS alarm monitor station been installed to Underwriters Laboratories certified standards?			<input type="checkbox"/> Yes <input type="checkbox"/> No
<i>Contractor facility submit copy of Certificate</i>			
g. Has the IDS passed AO or UL 2050 installation and acceptance tests?			<input type="checkbox"/> Yes <input type="checkbox"/> No
<i>If yes, attach a copy of certificate (Non-commercial proprietary system must answer all questions)</i>			
h. High Security Switches Type I			<input type="checkbox"/> Yes <input type="checkbox"/> No
i. High Security Switches Type II			<input type="checkbox"/> Yes <input type="checkbox"/> No
j. Motion sensor (indicate sensor placement on a legible floor)			
k. Are any other intrusion detection equipment sensors/detectors in use?			<input type="checkbox"/> Yes <input type="checkbox"/> No
<i>Please identify make, model and manufacturer and function (indicate on floor plan)</i>			
Make	Model	Manufacturer	Function
l. Does the IDS extend beyond the SCIF perimeter?			<input type="checkbox"/> Yes <input type="checkbox"/> No
m. Can the status of PCU be changed from outside IDS protection?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, is an audit conducted daily?			<input type="checkbox"/> Yes <input type="checkbox"/> No
n. Do any intrusion detection equipment components have audio or video capabilities?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, please explain.			
o. PCU administrator SCI indoctrinated?			<input type="checkbox"/> Yes <input type="checkbox"/> No
p. Is external Transmission Line Security used?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, please explain.			
q. What is the method of line security? National Institute of Standards and Technology (NIST) FIBS AES encryption?			<input type="checkbox"/> Yes <input type="checkbox"/> No
1) If yes, has the encryption been certified by NIST or another independent testing laboratory?			<input type="checkbox"/> Yes <input type="checkbox"/> No
2) If not NIST standard, is there an alternate?			<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, please explain.			

CLASSIFICATION

CLASSIFICATION

4) Does the alternate line utilize any cellular or other Radio Frequency (RF) capability?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
Manufacturer		Model Number	
r. Does any part of the IDS use local or wide area network (LAN/WAN)?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
1) Is the host computer dedicated solely for security purposes?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
2) Is the host computer secured within an alarmed area at the SECRET or higher level?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
3) Is the host computer protected through firewalls or similar devices?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> 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?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
5) Is the password changed semi-annually?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
6) Are remote security terminals protected the same as the host computer?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If no, please explain:			
2. Is emergency power available for the IDS?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
Generator?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If yes, how many hours?	
Battery?	<input type="checkbox"/> Yes <input type="checkbox"/> No	If yes, how many hours?	
3. Where is the IDS alarm monitor station located?			
4. Does the monitor station have any remote capabilities (i.e., resetting alarms, issuing PINs, accessing/securing alarms, etc.?)		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
If yes, please explain:			
5. Does the IDS have any automatic features (i.e., timed auto-secure, auto-access capabilities?)		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
6. Does the PCU/keypad have dial out capabilities?		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
7. IDS response personnel		<input type="checkbox"/> Yes	<input type="checkbox"/> No <input type="checkbox"/> N/A
a. Who provides initial alarm response?			
b. Does the response force have a security clearance?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ If yes, what is the clearance level?	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret
c. Do you have a written agreement with external response force?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Emergency procedures documented?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
e. Response to alarm condition:	Minutes		
f. Are response procedures tested and records maintained?		<input type="checkbox"/> Yes	<input type="checkbox"/> No
If no, please explain:			
g. Has a catastrophic failure plan been approved by the CSA?		<input type="checkbox"/> Yes	<input type="checkbox"/> No

CLASSIFICATION

■ If no, please explain:

10. REMARKS:

Section F: Telecommunication Systems and Equipment Baseline

1. 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

2. 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 specific location of the CTS

3) Is the facility protecting the CTS physically controlled?

■ If yes, what is the clearance level (if any) of facility or area where the switch is located. SCI Top Secret Secret

■ If no facility clearance level how is the facility or area where the switch is located controlled?

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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
6) Is an up-to-date master copy of the CTS software program maintained for confirmation and/ or reloading of the operating system?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
7) Does the CTS have the capability to force or hold a telephone station off-hook?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
8) Does the CTS use remote maintenance and diagnostic procedures or other remote access features?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<ul style="list-style-type: none"> ■ If yes, explain maintenance procedures 			
9) Do the CTS installers and programmers have security clearances?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<ul style="list-style-type: none"> ■ If yes, at what access level (minimum established by AO) 	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret
<ul style="list-style-type: none"> ■ If no, are escorts provided? 	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
d. Is it a Voice over Internet Protocol (VOIP) phone system (IPS) (Ref CNSSI 5000)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> 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)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
<ul style="list-style-type: none"> ■ If no, please explain? 			
3) Is access to the facility housing the IPS physically controlled?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<ul style="list-style-type: none"> ■ If yes, what is the clearance level (if any) of facility or area where the switch is located and how is the area controlled? 	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret
<ul style="list-style-type: none"> ■ 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	
<ul style="list-style-type: none"> ■ If no, please explain? 			

CLASSIFICATION

5) Are all program media, such as tapes and/ or disks, from the IPS afforded physical protection from unauthorized alterations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
6) Is an up-to-date master copy of the IPS software program maintained for confirmation and/ or reloading of the operating system?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
7) Does the IPS have the capability to force or hold a telephone station off-hook?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
8) Does the IPS use remote maintenance and diagnostic procedures or other remote access features?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
9) Do the IPS installers and programmers have security clearances?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ If yes, at what access level (minimum established by AO)?	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret
■ If no, are escorts provided?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

3. Automatic telephone call answering

a. Are there any automatic call answering devices for the telephones in the SCIF?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
1) If yes, please identify the type		
■ Voicemail/ unified message service?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ Standalone telephone answering device (TAD)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
2) Provide manufacturer and model number of the equipment		
Manufacturer	Model	
b. Are speakerphones/ microphones enabled?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ If yes, has the remote room monitoring capability been disabled?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ Has this been approved for use by the AO?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
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 tone?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

4. Are any multi-function office machines (M-FOMs) used within the SCIF (M-FOMs are electronic equipment that can be used at network or standalone printers, facsimiles, and copiers)?

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.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Make	Model	Serial Number
b. If yes, please identify all features and information processing level of each M-FOM		
1) Copier?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ If yes, level(s) of information	<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret
	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified

CLASSIFICATION

2) Facsimile?				<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
■ If yes, level(s) of information		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
3) Printer? (connected to a standalone computer or network)				<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
■ If yes, please explain and identify the system(s) and the level(s) of information						
System:		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
System:		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
System:		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
System:		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
System:		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
c. Does the M-FOM have memory storage capability?				<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
If yes, what kind?		<input type="checkbox"/> Volatile (information in memory clears/ erases when powered off)		<input type="checkbox"/> Non-volatile (information in memory that remains when powered off)		
d. Does the M-FOM have a digital hard drive?				<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
e. Have maintenance and disposition procedures been established?				<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
f. Does the M-FOM have voice transmission capability and/ or a telephone handset?				<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
■ If yes, describe how is this feature protected?						
5. Are there any video teleconference (VTC) systems installed?					<input type="checkbox"/> Yes	<input type="checkbox"/> No
■ If yes, what level(s) of information is the VTC system processing?		<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Unclassified	
Which room(s) contain VTC systems?						
6. Are there any commercial television receivers installed?					<input type="checkbox"/> Yes	<input type="checkbox"/> No
<i>If yes, provide a separate annotated floor plan of the commercial television system</i>						
7. Does the SCIF have any automated environmental infrastructure systems?					<input type="checkbox"/> Yes	<input type="checkbox"/> 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)						
8. REMARKS:						

Section G: Acoustical Protection

1. Do all areas of the SCIF meet AO required acoustical protection standards”? (Ref: Chapter 9A)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
---	------------------------------	-----------------------------

<ul style="list-style-type: none"> ■ 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. Are there any amplified audio systems used for classified information? (Example VTC, PA systems, etc.)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
--	------------------------------	-----------------------------

<ul style="list-style-type: none"> ■ 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? 	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
---	------------------------------	-----------------------------	-------------------------------

3. Is there a public address or music system entirely contained within the SCIF?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
---	------------------------------	-----------------------------

If yes, provide a separate annotated floor plan for each system

4. Is the SCIF equipped with a public address, emergency/fire announcement or music system originating outside the SCIF?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
---	------------------------------	-----------------------------

5. 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?	<input type="checkbox"/> Yes	<input type="checkbox"/> 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)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No	<input type="checkbox"/> N/ A
--	------------------------------	-----------------------------	-------------------------------

2. REMARKS:

Section I: INFOSEC/TEMPEST/Technical Security

1.	Does the facility electronically process classified information? (Ref: Chapter 13)	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	■ If yes, complete TEMPEST CHECKLIST FOR SCIF Form		