(CLASSIFICATION)

Intelligence Community Policy Guidance 705.1 (Attachment A)

Form version date: 31 October 2008

Fixed Facility Accreditation Checklist for [Insert Org Name]

[Date]

[Address]

(CLASSIFICATION)

General Guidance

When completing a FFC, all questions shall be answered. If an area or question does not apply list "N/A" or "None".

For FFC page changes submit a complete and updated FFC with diagrams/attachments to DIA/DAC-2A2 indicating all changes with the placement of an asterisk (*) beside all information that has changed prior to requesting accreditation.

All DIA accredited SCIFs shall comply with the requirements of ICD 705, Physical Security, its implementing Intelligence Community Policy Guidance (ICPGs) and the Sensitive Compartmented Information, Administrative Security Manual, DoD 5105.21-M-1.

ICD 705 implementing ICPGs include:

- **ICPG 705.1: Forms**
- **ICPG 705.2: Construction of SCIFs Within the United States (also covers U.S. Thrust, Territories and Possessions)**
- **ICPG 705.3: Construction of SCIFs Outside the U.S.**
- **ICPG 705.4: Tactical SCIFs**
- **ICPG 705.5: Portable Electronic Devices (PEDs)**
- **ICPG 705.6: Acoustic Control and Sound Masking Techniques for SCIFs**
- **ICPG 705.7: Intrusion Detection Systems**
- **ICPG 705.8: Personnel Access Control for SCIFs**
- **ICPG 705.9: Telecommunications Systems and Equipment**
- **ICPG 705.10: SCIF Administrative Controls**

ICD 700.1, Security Glossary provides definitions of terms associated with security issues.

FFC's will normally be classified CONFIDENTIAL. Where appropriate FFC's may be classified at a higher level where other guidance applies.

Requests for exceptions or waivers shall be coordinated in advance with DAC-2A2. When requesting an exception or waiver, elements shall follow the guidelines in the DoD 5105.21-M-1. Exceptions and waivers will be considered on a case-by-case basis, with the CSA, DAC-2A2, being the final arbitrator.

When developing FFCs, DoD elements are strongly encouraged to coordinate questions or issues with DAC-2A2. Construction of SCIF's may not begin until after the pre-construction FFC has been approved by DAC-2A2.

(*Classify and date appropriately when filled in*)

Intelligence Community Policy Guidance 705.1

Attachment A

SCIF Fixed Facility Accreditation Checklist

(Effective upon publication date TBD)

CHECK Applicable blocks			
☐ Pre-construction	☐ Initial Facility Accreditation	☐ Facility Modification	☐ Administration Page Change
☐ New Facility	☐ Re- Accreditation		

Checklist Contents

List of Attachments

(Diagrams must be submitted on 8 ½" x 11" or 11" x 17" format)

Section A: General Information				
1.	**SCIF Data**			
	Organization/Company Name	List your full unit, organization or company name.		
	SCIF Identification Number *(if applicable)*	List your DIA SCIF Identification Number assigned by DIA to include dashes (XX-XX-XXX). If an identification number has not been assigned by DIA state NONE in this space. DIA SCIF Identification Numbers are normally not assigned to new facilities until after the Concept Approval has been obtained and the pre-construction FFC has been submitted to DIA/DAC-2A2.		
	Organization subordinate to *(if applicable)*	List your Higher Headquarters/MAJCOM or servicing SSO.		
	Contract Number & Expiration Date *(if applicable)*	If the SCIF is going to be a contractor SCIF, list contract number and expiration date. Both items can be found on the valid DD Form 254. If the SCIF is going to be a government SCIF insert: Government SCIF – no contract number or expiration date.		
	Concept approval Date/by *(if applicable)*	List date Concept Approval was given and name of person/organization that approved the concept document. Heads of Military Intelligence Elements (HMIEs) or Senior Intelligence Officers (SIOs) of Combatant Commands and Defense Agencies are authorized to grant concept approval to establish a SCIF, including contractor SCIFs. This authority cannot be delegated to a lower command.		
	Cognizant Security Authority (CSA)	List DIA unless prior exception has been approved by DIA/DAC-2A2. Within DoD, DIA is the CSA for all SCIFs less NSA, NRO and NGA.		
	Defense Special Security Communication System Information ***(if applicable)***			
	DSSCS Message Address	List your DSSCS message address. If you do not know this, contact you're servicing SSO to obtain it.		
	DSSCS INFO Address	List your DSSCS INFO address. If you do not know this, contact you're servicing SSO to obtain it.		
	If no DSSCS Message Address, please provide passing instructions	If you do not have a DSSCS Message Address, list how you want communications forwarded to you (i.e. JWICS, SIPRnet, NIPRnet, secure communication/fax, etc.).		
2.	**SCIF Location:** List physical street address of SCIF in blocks below. If requested information does not apply list N/A. Rooms within SCIF perimeter boundaries, all inclusive, should be listed.			
	Street Address			
	Building Name/#		Floor(s)	
	Suite(s)		Room(s) #	

	City		Base/Post			
	State/Country		Zip Code			
3.	**Mailing Address (if different from SCIF location)** List mailing address, if used. List "Same" if information is the same as in block 2 above.					
	Street or Post Office Box					
	City		State		Zip Code	
4.	**E-Mail Address** List applicable JWICS, SIPRnet, NIPRnet email address and others along with the network/system name and level of classification approved for (i.e.; XXXXXXX@dia.ic.gov JWICS/TS/SCI). JWICS is the preferred method for communication with DIA.					
	Classified		(Network/System Name & Level)			
	Unclassified		(Network/System Name)			
	Other		(Network/System Name)			
5.	**Responsible Security Personnel** All Blocks Must be completed. Your are required to have a Primary and Alternate security officer.					
		PRIMARY		**ALTERNATE**		
	Name	List full name and rank if in the military.		List full name and rank if in the military.		
	Commercial Telephone	List commercial telephone number.		List commercial telephone number.		
	DSN Telephone	List DSN telephone number. If none list "None".		List DSN telephone number. If none list "None".		
	Secure Telephone	List secure telephone number.		List secure telephone number.		
	STU/STE Other Telephone	List STU/STE or other telephone numbers.		List STU/STE or other telephone numbers.		
	Home	List home telephone number for emergency use.		List home telephone number for emergency use.		
	Secure Fax	List secure fax telephone numbers(s) If none list "None".		List secure fax telephone numbers(s) If none list "None".		
	Command or Regional Special Security office/Name (SSO) *(if applicable)* List your SSO's name.					
	Commercial Telephone	List your SSO's primary commercial telephone number.		List an alternate commercial telephone number. If none list "None".		
	Other Telephone	List other telephone numbers for your SSO (STU/STE/secure). Secure telephone numbers are desired.		List other telephone numbers for your SSO (STU/STE/secure). Secure telephone numbers are desired.		
	Information Assurance Manager (IAM): Required in accordance with DoDIIS/CRYPTO SCI Information Systems Security Standards, if automated information systems (computers, PEDs, etc.) are used within the SCIF					
	Name:	List the name of your IAM.		List the name of your alternate IAM.		
	Commercial Telephone	List your IAM's commercial telephone number.		List your alternate IAM's commercial telephone number.		
	Secure Telephone	List your IAM's secure telephone number.		List your alternate IAM's secure telephone number.		
6.	**Accreditation Data**					
	a. Category/Compartments of SCI Requested: List SCI compartments (e.g. SI/TK/G/HCS) you					

	are requesting in this area when submitting initial concept approval request or when requesting re-accreditation. 1) Indicate storage requirement: Select only one: If closed storage is requested all SCI must be stored in GSA approved containers to include computer memory. When open storage is requested storage of SCI in GSA approved containers is not required (includes computer memory). If Continuous Operations (24/7 operations) is requested, the capability shall exist for storage of all SCI in GSA approved security containers is required unless facility meets Open Storage construction requirements (i.e. alarms, enhanced wall construction, etc). None should be selected if you are establishing a Secure Working Area or a Temporary Secure Working Area.				
	☐ Open	☐ Closed	☐ Continuous Operation		
	2) Indicate the facility type Select One: A Temporary Secure Working Area (TSWA) is a temporary facility that is used less than 40 hours per month (up to 12 months) for discussion and /or processing of SCI. SCI may not be stored in a TSWA. A Secure Working Area (SWA) is used for the discussion and/or processing of SCI, but where SCI may not be stored. Tactical SCIF's are temporary in nature (up to 12 months) and designed to support temporary operations that do not justify/support a permanent SCIF. See ICPG 705.4 for additional details relating to Tactical SCIFs. Most SCIFs will be considered Permanent SCIFs. When planning a Tactical SCIF that you believe will be in operation for more than one year, you should build this SCIF to permanent SCIF standards.				
	☐ Permanent	☐ Temporary Secure Working Area	☐ Secure Working Area	☐ Tactical	
	b. Existing Accreditation Information ***(if applicable)***				
	1) Category/Compartments of SCI:	List the SCI compartments your SCIF is approved for (i.e.; SI/TK/HCS etc).			
	2) Accreditation granted by: List the full name of the Agency that accredited your SCIF.	On: List the date your SCIF was accredited.			
	3) Waivers: List all waivers approved by the CSA. This information can be found in your SCIF administrative records or obtained from your CSA.				
	4) Co-Use Agreements	☐ Yes	☐ No	If yes, provide sponsor/compartment: If you have co-utilization agreement(s) in place identify the sponsoring Agency and the SCI compartments associated with each co-use agreement.	
	c. SAP(s) co-located within SCIF	☐ Yes	☐ No	If yes, identify SAP Classification level (check all that apply)	
	☐ SCI	☐ Top Secret	☐ Secret	☐ Confidential	
	d. SCIF duty hours	(hours to hours) Identify the hours per day your SCIF is operational. (i.e.; 06:00-20:00 hrs).		days per week List the days per week the SCIF will be operational (i.e.; Monday – Saturday)	
	e. Total square footage that the SCIF occupies				
	f. Has CSA issued any waivers? Answer Yes if a waiver has been issued. Answer No if there are no waivers.	☐ Yes	☐ No	☐ N/A	If yes, attach a copy of the waiver Attach a copy of each waiver authorized. Waivers must be reviewed annually by DIA/DAC-2A2 per DoD 5105.21-M-1.
	Construction/Modification If you are only submitting a page change select N/A.				

	Is construction or modification complete?	☐ Yes	☐ No	☐ N/A	If no, enter the expected date of completion
7.	**Inspections**				
	a. TSCM Service completed by		List organization, POC and telephone.		On _____ *(Attach a copy of report)*
	Were deficiencies corrected?	☐ Yes	☐ No	☐ N/A	If no, explain
	b. Last physical security inspection by		List organization, POC and telephone.		On _____ *(Attach a copy of report)*
	Were deficiencies corrected?	☐ Yes	☐ No	☐ N/A	If no, explain
	c. Last Staff Assistance Visit by: List Agency that conducted the last staff assistance visit.				_____ *(Attach a copy of report)*
8.	**REMARKS:** Include any additional remarks you would like included that are associated with Section A, General Information				

Section B: Peripheral Security (Peripheral security are physical measures in place external to the building that houses the SCIF and extends to the farthest point under government or facility owner control.)					
1.	**Describe building exterior security**				
	a. Is building located on a controlled compound? (U.S. Government, Foreign Government or U.S. Contractor Compound)			☐ Yes	☐ No
	b. Fence Type	List type of fence (chain link, wood, etc), weight of fabric where appropriate (i.e.; 9 gauge 2 inch mesh), and location (around building/compound, etc)	Height Feet or meters.	Length Feet or meters	
	c. Fence Alarm	If yes, list details about fence alarms (i.e.; make, model. manufacturer, location of alarms, condition, installation date, who maintains alarm, location of monitoring station, who monitors alarms (U.S. citizens/foreign nationals, do they hold a security clearance), response time, response procedures to include who responds (primary/backup response force), power source to include backup power. If no fence alarm, state there is no fence alarm.			
	d. Fence Lighting	List details to include type, locations, candle power, distance apart, how lights are installed, how effective lights are illuminating compound perimeter, power source to include backup power.			
	e. Building Lighting	List details to include type, locations, candle power, distance apart, how lights are installed, how effective lights are illuminating building perimeter, power source to include backup power.			
	f. Cameras/Television (CCTV) *(include monitor location)*	List details about compound CCTV (i.e.; make, model. manufacturer, location of cameras (perimeter coverage, building coverage, SCIF coverage), condition, installation date, who monitors/maintains cameras, location of monitoring station, who monitors alarms (U.S. citizens/foreign nationals, do they hold a security clearance), response time to an unwanted event, response procedures to include who responds (primary/backup response force), power source to include backup power. If no CCTV, state there is no CCTV.			
	g. Guards	☐ Yes If yes, are they stationed in one place (static) or do they move around (roving).	☐ No	☐ Static Identify static position.	☐ Roving Identify roving patrol areas and extent of responsibilities.
	Clearance level of guards *(if applicable)*	List clearance level of guards (U.S. or foreign government clearance – Confidential, Secret, Top Secret. SCI Access). If no clearance state No Clearance.			
	During what hours/days?				
	Any SCIF duties?	☐ Yes	☐ No	If yes, describe duties List any duties away from the SCIF area.	
2.	**Building** *(Please provide legible general floor plan of the SCIF perimeter on a 8 ½" x 11" or 11" x 17" format) Include*				

	building diagram showing exterior of building and SCIF location within the building.					
	a. Construction type	List material used and thickness of exterior building walls (i.e. concrete block 8 inches thick).				
	b. Windows	List type, material used and thickness of exterior building windows (i.e. double pain class, use of security grills, locks, alarms etc.).				
	c. Doors	List type, material used and thickness of exterior building doors (i.e. double pain class, wood, metal, use of security grills, locks, alarms, etc.).				
	d. Describe access controls Automated or non-automated (i.e., card swipe and PIN, proximity, bio-metrics, key control, etc.)	Continuous If the building has access control procedures at all times (24/7) then they are continuous.	☐ Yes	☐ No	If no, during what hours?	
	e. Interior building guards Provide details regarding the guard force (citizenship, clearance level, number on duty at any given time, summary of responsibilities).	☐ Yes	☐ No	☐ Static Identify static position.	☐ Roving Identify responsibilities.	
	Clearance level of guards *(if applicable)*	List clearance level of guards (U.S. or foreign government clearance – Confidential, Secret, Top Secret. SCI Access). If no clearance state No Clearance.				
	During what hours/days	List hours/days guards are present on the compound or at the SCIF.				
	f. Building alarmed *(not SCIF)*	☐ Yes	☐ No	If the building alarm is separate from the SCIF alarm, provide details to include type of system/ equipment, sensor locations on building perimeter, who monitors/maintains, who responds, response time, etc.		
3.	**Security In-Depth**					
	What external security attributes and/or features should the CSA consider before determining whether or not this facility has Security In-Depth? Please identify/explain all factors: Security In-Depth is defined as a concept of security calling for layered and complementary controls sufficient to detect and deter infiltration and exploitation of an organization, its information systems and facilities. This is one of the determining factors on whether you will be granted Open or Closed storage and if you will be eligible for any waivers from ICD 705 standards. List all security features you think make up/enhance security in-depth surrounding your SCIF. Examples include, but are not limited to: Government or contractor controlled compound; fences; access control at the compound or building perimeter; exterior lighting/alarms/CCTV; guard force with static/roving patrols, quick response times; etc. For security in-depth to be effective you facility must have the capability to detect and respond to penetrations at the outer ring(s) (i.e.; having a compound perimeter fence that anyone can climb over with limited or no chance of detection does not constitute a layer of security in-depth.) To be effective and count toward security in-depth, proposed features must deter, delay and offer a reasonable probability of detection.					

Section C: SCIF Security

1. How is access to the SCIF controlled?

a. By Guard Force	☐ Yes	☐ No	If yes, what is their security clearance level? If SCI access is required identify the category (i.e.; SI, TK, etc.)
Is Guard Force Armed?	☐ Yes	☐ No	
b. By assigned personnel	☐ Yes	☐ No	If yes, how do personnel have visual control of SCIF entrance door?
Are Guards or personnel armed?	☐ Yes	☐ No	
c. By access control device	☐ Yes	☐ No	If yes, what kind? List identifying information (name, model number, manufacturer). Access control devices must be approved by the CSA.

☐ Automated access control system ☐ Non-automated

If non-automated (proximity badge, mechanical cipher) Answer the following questions if your access control system is non-automated.

1. Is there a by-pass key?	☐ Yes	☐ No	☐ N/A
If yes, how is the by-pass key protected?	Explain how the by-pass key is protected and where it is stored. Unless approved by the CSA by-pass keys shall be stored in another SCIF and controlled at all times by SCI cleared personnel.		
2. Manufacturer List the manufacturer's name of the access control device you are using.	Model List the manufacturers model number of the access control device you are using.		

(Attach sheet if additional space is required for this information)

If automated (Two part authentication i.e., badge/pin, bio-metric)

1. Are access control transmission lines protected by 128-bit encryption?

☐ Yes	☐ No	If no, explain the physical protection provided (i.e.; embedded in rigid conduit, etc.)

2. Is automated access control system located within a SCIF or an alarmed area controlled at the **SECRET** level? (This applies to badging machines and control computers). If No, explain where your access control system is located and why. A No answer will require a waiver and CSA approved mitigation.	☐ Yes	☐ No
3. Is the access control system encoded and are ID data and PINs restricted to SCI-indoctrinated personnel? (This applies to badging machines and control computers).	☐ Yes	☐ No Explain your answer
4. Do external access control outside SCIF have tamper protection?	☐ Yes	☐ No

					Explain your answer
	5. Is the access control device integrated with an IDS? Explain your answer giving details on how the system works.	☐ Yes	☐ No	☐ N/A	
	6. Is the access control device integrated with a network system? Explain your answer giving details on how the system works.	☐ Yes	☐ No	☐ N/A	
2.	**Does the SCIF have windows?** If yes, provide a description of SCIF windows (glass thickness, number of pains, film type (blast, RF, IR etc), etc.			☐ Yes	☐ No
	a. Are they acoustically protected?	☐ Yes	☐ No	☐ N/A	If yes, how? Please explain Explain how acoustic protected is maintained (thickness of glass, control of surrounding area, etc.)
	b. Are they secured against forced entry?	☐ Yes	☐ No	☐ N/A	If yes, how? Please explain Explain how force protection is maintained (type of glass, type of window film, iron bars, etc.)
	c. Are they protected against visual surveillance?	☐ Yes	☐ No	☐ N/A	If yes, how? Please explain Explain how (drapes, blinds, etc.)
3.	**Do ventilation ducts penetrate the SCIF perimeter?**			☐ 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, indicate how are they protected?				
	☐ IDS (Describe in Section E)	☐ Bars/Grills/Metal Baffles		☐ Other, please explain	
	b. Inspection ports? *(Ducts over 96 square inches require an inspection port that provides for visual observation of the physical barrier.)*	☐ Yes		☐ No	
	If yes, are they within the SCIF?	☐ Yes		☐ No	
	If not within the SCIF, are they secured?	☐ Yes	☐ No	Please explain how inspection port is secured (GSA approved padlock, key lock, etc.) Provide details of locking mechanism.	
	c. Do all ventilation ducts penetrating the perimeter meet acoustical requirements? Acoustic protection requirements are normally STC 45 unless amplified voice is used. If amplified voice is used STC 50 is required.			☐ Yes	☐ No
	*(**NOTE:** All ducts and vents, regardless of size may require acoustical protection)*				
	If yes, how are they protected? Check the appropriate block below to identify how acoustic protection is maintained.				
	☐ Metal baffles	☐ Noise generator	☐ Z-duct	☐ Other (describe)	
4.	**Construction Where possible submit example photographs of wall construction with the FFC. Permission to take photographs within your SCIF can be obtained from the servicing SSO (DoD 5105.21-M-1, Chapter 5).**				

	a. Perimeter wall material and thickness	List material used and thickness of walls. See ICD 705 for approved wall types.	
	Do the walls extend from true floor to true ceiling?	☐ Yes	☐ No
	b. True ceiling (material and thickness)	List material used and thickness of true ceiling.	
	c. False ceiling?	☐ Yes	☐ No
	If yes, what is the type of ceiling material?		
	What is the distance between false and true ceiling?	Answer question in feet and inches (i.e.; 1 foot 6 inches).	
	d. True floor (material and thickness)	List material used and thickness of true floor.	
	e. False floor?	☐ Yes	☐ No
	If yes, what is the type of false flooring?		
	What is the distance between the false and true floor?	Answer question in feet and inches (i.e.; 1 foot 6 inches).	
5.	**REMARKS** Provide any additional information you feel the CSA should be aware of relating to construction of the SCIF.		

Section D: Doors					
1.	**Describe SCIF primary entrance door construction (indicate on floor plan)** Identify number, thickness of door and building material (wood or steel doors) used.				
	a. Is there a day door? If yes, explain how the day and primary doors are configured.			☐ Yes	☐ No
	b. Does the door and doorframe meet sound attenuation requirements?			☐ Yes	☐ No
	If no, have acoustical countermeasures been employed?	☐ Yes	☐ No	If no, explain why countermeasures have not been applied. If countermeasures have been implemented (i.e.; vestibule) explain what they are and how they have been implemented.	
	c. Is an automatic door closer installed?	☐ Yes	☐ No	If no, explain why it has not been installed and any mitigation implemented.	
	d. Is a door sweep/thresholds installed?	☐ Yes	☐ No	If no, explain why it has not been installed and any mitigation implemented.	
	e. Is an acoustical/astragal strip installed?	☐ Yes	☐ No	If no, explain why it has not been installed and any mitigation implemented.	
2.	**Describe number and type of doors used for SCIF emergency exits and other perimeter doors including day access (show on floor plan)** Identify number, thickness of door and building material (wood or steel doors, etc.) used.				
	a. Do the doors and doorframes meet sound attenuation requirements?			☐ Yes	☐ No
	If no, have acoustical countermeasures been employed?	☐ Yes Explain type of countermeasure.	☐ No Explain why not.	☐ N/A If no countermeasures are needed.	
	b. Has exterior hardware been removed from emergency exit doors?	☐ Yes	☐ No Explain why not.		
3.	**Describe how the door hinges exterior to the SCIF are secured against removal (if in an uncontrolled area)** (i.e.; welded, set screws, or fixed in a manner that prevents removal). If this does not apply specifically state that all perimeter door hinges are located within the SCIF.				
4.	**Locking devices**				
	a. Does primary SCIF entrance door meet GSA Specification FF-L 2740A ☐ Yes ☐ No				
	1. List combination lock manufacturer, model number and group rating				
	Manufacturer	**Model Number**	**Group Rating**		

	Fill in this section.	Fill in this section.		Fill in this section.
	2. Does the entrance door stand open into an uncontrolled area?	☐ Yes	☐ No	If yes, please describe tamper protection for locking device.
	b. Emergency exits and other perimeter doors: Describe (locks, metal strip/bar, deadbolts, local annunciation, and panic hardware) Describe type of locking hardware used to protect emergency doors. Locking device must include deadlocking panic hardware on the interior side of the SCIF.			
	c. Where is the lock combination(s) filed? (Please identify the SCIF CSA and SCIF ID #) Combinations are not authorized to be stored outside of a SCIF. If there are no other SCIFs in your operations area, contact DAC-2A2 for assistance in storage of your SCIF combination.			
5.	**REMARKS** Provide any additional information you feel the CSA should be aware of relating to SCIF perimeter doors.			

Section E: Intrusion Detection Systems

1. General IDS Description **Provide a SCIF floor plan outlining placement of all alarm sensors and zones that are included within the SCIF alarm system (preferably on a piece of paper measuring 8 ½ by 11 inches).**

a. IDS company provider name *(if applicable)*			List the full name and address of the company that installed the SCIF alarm system. This may be different from the company or organization that monitors the alarms. In this section we want to know who installed the alarm system.		
b. Premise Control Unit (PCU)					
Manufacturer	**Model Number**	Tamper Protection		☐ Yes	☐ No Explain why not.
c. Is the PCU located inside the SCIF perimeter (indicated on floor plan?)		☐ Yes	☐ No	If no, please explain where it is located. Per ICD 705, PCU shall be located within the SCIF unless a waiver is approved by the CSA. If the SCIF PCU is located outside the SCIF contact DAC-2A2 for guidance.	
d. Location of Balanced Magnetic Switches			On a SCIF floor plan identify the location of all Balanced Magnetic Switches (BMS). Coverage and installation must comply with ICPG 705.7, Intrusion Detection Systems.		
Manufacturer	Model Number	Tamper Protection		☐ Yes	☐ No If No explain why.
Accessible points of entry / perimeter? Does BMS cover all accessible points of entry/exit to the SCIF?				☐ Yes	☐ No If No explain why.
e. Has the IDS alarm monitor station been installed to Underwriters Laboratories certified standards?				☐ Yes	☐ No If No explain why.
If yes, provide certification number and expiration date of UL Certification. This information can be obtained from the company that installed the alarm system. **For contract facilities, the UL2050 certificate is mandatory. Government facilities are required to install/test IDS to meet UL2050 standards but are not required to obtain certificate.**		**Certification Number**		**Expiration Date**	
f. Has the IDS passed CSA or UL 2050 installation and acceptance tests?				☐ Yes	☐ No If No explain

				why.
	g. Motion sensors (indicate sensor placement on a legible floor plan; 8 ½" x 11" or 11' x 17" paper) Identify placement of all motion sensors on floor plan			
	1. Manufacturer	List alarm sensor manufacturer(s)		
	2. Model number	List model numbers for all alarm sensors		
	3. Tamper protection		☐ Yes	☐ No If No, explain why.
	4. Do the motion sensors cover all accessible points of entry on the perimeter of the SCIF?		☐ Yes	☐ No If No, explain why.
	5. Do the motion sensors cover all areas where SCI is stored?		☐ Yes	☐ No If No, explain why.
	6. Are motion sensors installed above the false ceiling?	☐ Yes	☐ No	☐ N/A
	7. Are motion sensors installed below the false floors?	☐ Yes	☐ No	☐ N/A
	h. Are any other intrusion detection equipment sensors/detectors in use? (i.e.; glass break sensors, volumetric sensors, PDS sensors, etc.)		☐ Yes	☐ No
	Please identify make, model and manufacturer and function (indicate on floor plan) If Yes complete the below information for each type of sensor used within your SCIF			
	Make Fill in this section if applicable.	**Model** Fill in this section if applicable.	**Manufacturer** Fill in this section if applicable.	**Function** Fill in this section if applicable (i.e.; door/window contact, etc)
	i. Does the IDS extend beyond the SCIF perimeter? (i.e. outside the perimeter walls of the SCIF).		☐ Yes Provide details.	☐ No
	j. Can the status of PCU be changed from outside IDS protection? (i.e. can the monitoring station, guard force or maintenance personnel turn alarms off or on, place them in maintenance mode, shunt alarms, etc. from outside the SCIF).		☐ Yes Provide details.	☐ No
	If yes, is an audit conducted daily?		☐ Yes Explain who conducts the audit and their clearance level.	☐ No If No explain why not.
	k. Has the IDS configuration been approved by the CSA?		☐ Yes	☐ No If No

			explain why not.
	l. Do any intrusion detection equipment components have audio or video capabilities?	☐ Yes If Yes provide details below.	☐ No
	If yes, please explain	Explain why intrusion detection equipment has audio or video capabilities. A waiver of ICD 705.7 standards is required if this capability exist.	
	Has the CSA granted a waiver for this capability? If yes, list the DTG of the message.	☐ Yes	☐ No
	m. IDS Administrator SCI indoctrinated?	☐ Yes	☐ No
	n. What is the method of External Transmission Line Security? (i.e., hard wired, RF transmission, other)		
	o. Is 128-bit or greater encryption used? Does the transmission line security have 128-bit (or greater) encryption?	☐ Yes	☐ No
	1) If yes, has the encryption been certified by National Institute of Standards and Technology (NIST) or another independent testing laboratory? (provide copy of NIST certificate for PCU listed 1.b above)	☐ Yes	☐ No
	2) If not 128-bit (or greater) encryption, is there an alternate? If 128-bit encryption is not available explain why and document proposed method to maintain line security and/or integrity of the IDS. When 128-bit encryption is not available alternatives should be discussed with and approved by DAC-2A2	☐ Yes	☐ No
	3) If yes, please explain	Explain how alternative method will maintain line security and/or integrity of the IDS.	
	4) Does the alternate line utilize any cellular or other Radio Frequency (RF) capability?	☐ Yes	☐ No

	Manufacturer List manufacturer if appropriate.	**Model Number** List model number if appropriate		
	p. Does any part of the IDS use local or wide area network (LAN/WAN)? If Yes provide a brief description of the LAN/WAN.	☐ Yes	☐ No	☐ N/A
	1) Is the network intrusion detection software (NIDS) administrator at least **TOP SECRET** (collateral) cleared? If No explain.	☐ Yes	☐ No	☐ N/A
	2) Is the host computer dedicated solely for security purposes? If the answer is No, explain other uses and how alarm functions are segregated from other functions performed by the computer.	☐ Yes	☐ No	☐ N/A
	3) Is the host computer secured within an alarmed area controlled at the **SECRET** or higher level? Explain where this area is located and who controls it.	☐ Yes	☐ No	☐ N/A
	4) Is the host computer protected through firewalls or similar devices? Explain your answer. If host computer is protected by firewalls or similar devices, identify them.	☐ Yes	☐ No	☐ N/A

	5) Is the password for the host computer unique for each user and at least 8-characters long?	☐ Yes	☐ No	☐ N/A
	6) Is the password changed semi-annually?	☐ Yes	☐ No	☐ N/A
	7) Are remote security terminals protected the same as the host computer? If No, explain how they are protected below.	☐ Yes	☐ No	☐ N/A
	If no, please explain — Fill in only if you responded No to Question 7 above.			
	n. Was the IDS installed by US citizens? Prior to using foreign nationals to install a SCIF IDS contact DAC-2A2.	☐ Yes	☐ No	☐ N/A
	If no, please explain who installed IDS to include name of personnel who installed, their citizenship, name and address of their employer.			
2.	**Is emergency power available for the IDS?** Emergency backup power for the SCIF and monitoring station shall be provided by battery, generator or both. If batteries are provided for emergency backup power, they shall provide a minimum of 24 hours (UL 2050) of backup power and they shall be maintained at full charge by automatic charging circuits. If generators are used for backup power, verify that the IDS automatically switches from commercial to generator power. Backup power supplies shall be tested periodically.	☐ Yes	☐ No	☐ N/A
	Generator?		☐ Yes	☐ No
	If yes, how many hours? — Answer this question if SCIF has emergency generator power. (i.e., on a full tank of fuel running at 80% capacity, the generator will provide x hours of backup power. Provide info on fuel reserve/capacity and type.) If SCIF does not have generator backup power insert N/A			
	Battery?		☐ Yes	☐ No
	If yes, how many hours? — Answer this question if SCIF has emergency battery power. If SCIF does not have battery backup power insert N/A.			
3.	**Describe the method of ventilation and duct work protection** *(if applicable from Annex A, Section 3C)* Answer this question for ventilation and duck penetrations of the SCIF perimeter exceeding 96 square inches.			
4.	**Where is the IDS alarm monitor station located?** — Provide address and name of organization/company monitoring the IDS			
5.	**Does the monitor station have any remote capabilities (i.e., resetting alarms, issuing PINs, accessing/securing alarms, etc?**	☐ Yes If Yes explain below.	☐ No	☐ N/A
	If yes, please explain — List remote capabilities and standard operating procedures for use.			
6.	**Does the IDS have any automatic features (i.e., timed auto-secure, auto-access capabilities?** If yes, provide a list of features that Answer this question if SCIF has emergency generator power. (i.e., on a full tank of fuel running at 80% capacity, the generator will provide x hours of backup power. Provide info on fuel reserve/capacity and type.) If SCIF does not have generator backup power insert	☐ Yes	☐ No	☐ N/A

	N/A.		
7.	**Does the PCU/keypad have dial out capabilities?** If yes, provide a list of features exist.	☐ Yes	☐ No
8.	**IDS response personnel**		
	a. Who provides initial alarm response?		
	b. Does the response force have a security clearance?	☐ Yes	☐ No
	If yes, what is the clearance level?		
	c. Do you have written agreement with external response force? Provide an overview of the agreement and attach.	☐ Yes	☐ No
	d. Emergency procedures documented? Provide overview and location(s) where procedures are documented.	☐ Yes	☐ No
	e. Response to an alarm condition:	____ Minutes	
	g. Are response procedures tested and records maintained? IDS testing is required semi-annually and records of such must be maintained.	☐ Yes	☐ No
	If no, please explain		
	h. If required, has a catastrophic failure plan been approved by the CSA? It is recommended that IDS Catastrophic Failure Plans be included in the SCIF Emergency Action Plan.	☐ Yes	☐ No If No explain.
9.	**Does the IDS undergo semiannual testing?** IDS testing is required semi-annually and records of such must be maintained.	☐ Yes	☐ No
10.	**Have IDS records been maintained?**	☐ Yes	☐ No
	If no, please explain	Only answer this question if answer to above question is No.	
11.	**REMARKS** Provide any additional information you feel the CSA should be aware of relating to the SCIF IDS.		

Section F: Telecommunication Systems and Equipment Baseline				
1.	**Is the facility declared a "No classified Discussion Area"?**		☐ Yes	☐ No
	If yes, then the audio protection questions within Section 2 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 Answer the remaining questions.	☐ No Mark all remaining questions as N/A and go to Section 3.
	What is the method of on-hook protection? One of the three methods must be Yes. What is the method of on-hook protection? if item 1 above is "YES", then sub-items 1, 2, 3, or 4 or any combination of these must be used			
	1. TSG-6 approved telephone or instrument If No explain your answer. Telephone Security Group (TSG) TSG-6, dated 1990, and updated January 2003, is a compilation of telephone security equipment that has been evaluated and approved by the TSG for use within SCIFs. TSG-6 applies to all telephone installations that must be provided with on-hook audio security.	☐ Yes	☐ No	☐ N/A
	(Please identify all telephone equipment/stations and/or instruments being used either below or as an attachment)			
	Manufacturer List manufacturer of telephones.	**Model Number** List model numbers of telephones.	**TSG Number** *(if applicable)* List TSC Number if applicable.	
	2. TSG-6 approved disconnect device? Does you telephone system have a TSG-6 approved disconnect device.	☐ Yes	☐ No	☐ N/A
	a) Line disconnect?	☐ Yes	☐ No	☐ N/A
	b) Ringer protection?	☐ Yes	☐ No	☐ N/A
	Manufacturer List manufacturer of ringer protection.	**Model Number** List model numbers of ringer protection.	**TSG Number** *(if applicable)* List TSG Number is applicable.	
	3. TSG-2 configured computerized telephone system (CTS)? If No explain your answer. TSG-2 provides guidelines for installation and operation of computerized telephones within SCIFs.	☐ Yes	☐ No	☐ N/A
	a) If yes, please provide the following information about the CTS:			
	Manufacturer List manufacturer of telephones.	**Model** List model numbers of telephones.		
	b) If yes, please provide specific location of the CTS			
	c) How is the facility protecting the CTS physically controlled?	Provide details.		
	d) If yes, what is the clearance level (if any) of facility or area where the switch is located and how is			

	area controlled?			
	e) Are all cables, signal lines and intermediate wiring frames between the SCIF telephones and the CTS physically protected within a physically controlled space?		☐ Yes	☐ No If No explain below.
	If no, please explain	Explain No answer to above question.		
	f) Are all program media, such as tapes and/or disks, from the CTS afforded physical protection from unauthorized alterations? Explain your answer. Where are they maintained, who has access to them, etc.		☐ Yes	☐ No
	g) Is an up-to-date master copy of the CTS software program maintained for confirmation and/or reloading of the operating system? If Yes where is master copy maintained at.		☐ Yes	☐ No
	h) Does the CTS have the capability to force or hold a telephone station off-hook? If yes, explain.		☐ Yes	☐ No
	i) Does the CTS use remote maintenance and diagnostic procedures or other remote access features?		☐ Yes	☐ No
	If yes, explain maintenance procedures	If yes, explain maintenance procedures.		
	j) Do the CTS installers and programmers have security clearances?		☐ Yes	☐ No
	If yes, at what access level (minimum established by CSA)			
	If no, are escorts provided?		☐ Yes	☐ No
	4. Does the Unclassified telephone system use a Voice over Internet Protocol (VoIP) phone system (Ref. CNSSI 5000)?	☐ Yes	☐ No	☐ N/A
	a) If yes, please provide the following information about the VoIP			
	Manufacturer List manufacturer of telephones.	**Model** List model numbers of telephones.	**IPS Location** List IPS location	
	b) 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, please explain	Explain why you do not have off-hook audio protection.		
	c) Is access to the facility housing the VoIP physically controlled? Explain where this facility is located.		☐ Yes	☐ No
	d) If yes, what is the clearance level (if any) of facility or area where the switch is located and how is the area controlled?			
	e) Are all cables, signal lines and intermediate wiring frames between the SCIF telephones and the VoIP physically protected or contained within a physically controlled space?		☐ Yes	☐ No
	If no, please explain	Explain why cables, signal lines and wiring between the SCIF and the VoIP are not physically protected or contained within a physically controlled space.		
	f) Are all program media, such as tapes and/or disks, from the VoIP afforded physical protection from unauthorized alterations?		☐ Yes	☐ No If No explain.

	g) Is an up-to-date master copy of the VoIP software program maintained for confirmation and/or reloading of the operating system?	☐ Yes	☐ No If No explain.
	h) Does the VoIP have the capability to force or hold a telephone station off-hook?	☐ Yes If Yes, explain.	☐ No
	i) Does the VoIP use remote maintenance and diagnostic procedures or other remote access features?	☐ Yes If Yes explain procedures.	☐ No
	j) Do the VoIP installers and programmers have security clearances?	☐ Yes	☐ No If No explain.
	If yes, at what access level (minimum established by CSA?		
	If no, are escorts provided?	☐ Yes	☐ No If No explain.

3.	**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 Identify all call answering devices			
	a. voice mail/unified message service	☐ Yes		☐ No
	b. Standalone telephone answering device (TAD)	☐ Yes		☐ No
	2) Provide manufacturer and model number of the equipment			
	Manufacturer **List manufacturer**	**Model Number** **List model number**		
	a. Are speakerphones/microphones enabled? If Yes, provide specific room location(s).	☐ Yes	☐ No	☐ N/A
	If yes, has the remote room monitoring capability been disabled?		☐ Yes	☐ No
	Has this been approved for use by the CSA?	☐ 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 tone?		☐ Yes	☐ No If No explain.
4.	**Are any multi-function office machines (M-FOMs) used within the SCIF (M-FOMs are electronic equipment that can be used as 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			
	Make List Make(s)	**Model** List Model Numbers	**Serial Number** List unit serial numbers	
	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	(CONFIDENTIAL, SECRET, TOP SECRET, SCI).		
	2) Facsimile?	☐ Yes	☐ No	☐ N/A
	If yes, level(s) of information	(CONFIDENTIAL, SECRET, TOP SECRET, SCI).		
	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) List systems and level of information (CONFIDENTIAL, SECRET, TOP SECRET, SCI)			
	c. Does the M-FOM have memory storage capability?		☐ Yes	☐ No
	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? Explain your answer if No.	☐ Yes	☐ No	☐ N/A
	f. If reproduction of classified/sensitive materials takes place outside the SCIF, describe equipment and security procedures used to reproduce documents			
	g. Does the M-FOM have voice transmission capability and/or a telephone handset?	☐ Yes	☐ No	☐ N/A
	If yes, how is this features protected? Please describe			
5.	**Are there any video teleconference (VTC) systems installed?**		☐ Yes	☐ No
	If yes, what level(s) of information is the VTC system processing? (CONFIDENTIAL, SECRET, TOP SECRET, SCI).			
	Which room(s) contain VTC systems?	Identify specific area/rooms within the SCIF		
6.	**Are there any commercial television receivers installed?**		☐ Yes	☐ No
	If yes, provide a separate annotated floor plan of the commercial television system. Provide 1) cable medium used for broadcast signal, 2) model/manufacturer of signal amplifier/attenuator 3) a separate annotated floor plan of the commercial television system outlining locations of all commercial television units and signal flow.			
7.	**Are all telecommunications systems, devices, features, and software documented? (Attached telecommunication baseline)**		☐ Yes	☐ No If No explain.
8.	**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) Be specific providing enough detail for evaluation of each system. If available provide manufacturer specifications/capabilities.			
9.	**REMARKS** Provide any additional information you feel the CSA should be aware of relating to the SCIF's telecommunication systems and equipment.			

Section G: Acoustical Protection				
1.	**Do all areas of the SCIF meet acoustical protection requirements of Annex E?** Requirements include STC 45 for normal conversation and STC 50 for amplified voice.		☐ Yes	☐ No
	If no, describe additional measures taken to provide conforming acoustical protection (e.g., added sound insulation, door and windows coverings, stand-off areas, sound masking, etc.) Provide countermeasures or mitigation strategy implemented, if acoustical requirements cannot be met through general SCIF construction.			
2.	**Are there any amplified audio systems used for classified information? (Example VTC, PA systems, etc.)** Provide details of each system.		☐ Yes	☐ No
	If yes, are the walls/ceilings/floor of the room where the amplified audio system resides acoustically treated to meet a Sound Transmission Class (STC) of 50 or better?	☐ Yes	☐ No If No, a mitigation strategy should be identified and implemented.	☐ N/A
3.	**Is there a public address or music system entirely contained within the SCIF?**		☐ Yes	☐ No
	If yes, provide a separate annotated floor plan for each system. Include manufacturer, model number, specifications and UL conformance data. NOTE: CSA Certified TEMPEST Technical Authority (CTTA) review may be required.			
4.	**Is the SCIF equipped with a public address, emergency/fire announcement or music system originating outside the SCIF?** If Yes, provide a separate annotated floor plan for each system indicating location of system isolation equipment. Include manufacturer, model number, specifications and UL conformance data. NOTE: CSA Certified TEMPEST Technical Authority (CTTA) review may be required.		☐ Yes	☐ No

Section H: Classified Destruction Methods					
1.	**Destruction methods**				
	a. Describe the method and equipment used for destruction of classified/sensitive material (if more than one method or device, use Remarks to describe. (If more than one device, use remarks to list all manufacturer and model) Equipment must be on the NSA approved list of destruction equipment.				
	Method Identify method (burn, shred, pulp, disintegrators, etc.)	**Device Manufacturer** Identify manufacturer	**Model** Identify model number		
	b. Is a secondary method of destruction available?			☐ Yes If yes identify method(s).	☐ No
	c. Describe the location of destruction site(s) in relation to the secure facility Describe distance in standard units (feet, meters, miles) and provide the street address, building number and room number if applicable for the alternate facility.				
	d. Describe method or procedure used for handling non-soluble classified/sensitive material at this facility Describe how you dispose of these items (I.e.; hard drives, CD-ROMs, DVDs, solid state media				
	e. Do you have a written Emergency Action Plan (EAP) approved by CSA (if required)? EAPs are mandatory per DoD 5105.21-M-1, Chapter 5. Does EAP cover emergency destruction? Include manufacturer, model number, specifications and UL conformance data. NOTE: CSA Certified TEMPEST Technical Authority (CTTA) review may be required. Include manufacturer, model number, specifications and UL conformance data. NOTE: CSA Certified TEMPEST Technical Authority (CTTA) review may be required.	☐ Yes	☐ No	☐ N/A	
2.	**REMARKS** Provide any additional information you feel the CSA should be aware of relating to emergency destruction equipment.				

Section I: INFOSEC/TEMPEST/Technical Security				
1.	**Does the facility electronically process classified information?**		☐ Yes	☐ No
	If yes, what compartments are processed? List Level and specific compartments (i.e.; TOP SECRET//SI//TK, etc)			
2.	**Are information processing systems Certified?** ☐ Yes ☐ No **Accredited** ☐ Yes ☐ No			
	Accreditation granted by: List agency	On List date of accreditation		
3.	**For the last TEMPEST Accreditation (if applicable), provide the following information**			
	Accreditation granted by: List agency	On List date of accreditation		
4.	**Has the CSA's Certified TEMPEST Technical Authority (CTTA) required any TEMPEST countermeasures?** Answer this question	☐ Yes	☐ No	☐ N/A
	If yes, please identify the countermeasures that have been installed (i.e. non-conductive sections, Radio Frequency (RF) shielding, power/signal line filters, window film, etc.) Answer this question if your CSA's CTTA required TEMPEST countermeasures for your SCIF.			
5.	**Are there any other systems installed within or in close proximity to the SCIF that have RF capability (e.g., fire alarm, ground-to-air-radio, cellular tower, RF networks, etc)?**		☐ Yes	☐ No
	If yes, please explain	Answer if appropriate. Provide details to include type and location.		

When submitting you FFC be sure to include the following attachments:

1. General floor plan/diagram (Section B, Item 2)
2. Ventilation Duct Penetration diagram (Section C, Item 3
3. Intrusion Detection System (IDS) diagram (Section E, Item 1)
4. Location of commercial television receivers diagram (section F, Item 6)
5. Public Address/Fire Announcement Floor Plan diagram (Section G, Item 4)
6. Telecommunications baseline (Section F, Item 7)