

SCIF Compartmented Area (CA) Fixed Facility Checklist

CHECK Applicable blocks		
<input type="checkbox"/> Initial Approval	<input type="checkbox"/> Re-approval	<input type="checkbox"/> Modified Facility
<input type="checkbox"/> Pre-construction	<input type="checkbox"/> New Facility	<input type="checkbox"/> Page Change

Checklist Contents

Section A: General information

Section B: Compartmented Area Security

Section C: Compartmented Area Type Descriptions

List of Attachments

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

Section A: General Information

1. SCIF Data

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

2. Location of Proposed Compartmented Area

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

3. Mailing Address (if different from SCIF location)

<i>Street or Post Office Box</i>		
<i>City</i>	<i>State ST</i>	<i>Zip Code</i>

4. Responsible Security Personnel

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

5. Existing SCIF Accreditation Data

a. Type					
<input type="checkbox"/> Open Storage	<input type="checkbox"/> Closed Storage	<input type="checkbox"/> IT Processing	<input type="checkbox"/> Discussions	<input type="checkbox"/> Continuous Operation	<input type="checkbox"/> Fixed <input type="checkbox"/> TSWA <input type="checkbox"/> SWA <input type="checkbox"/> Other
b. Accreditation Granted by:			on:		
c. If automated information system (AIS) is used, has an accreditation been granted?					<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, identify compartment classification level (check all that apply)					
<input type="checkbox"/> SCI	<input type="checkbox"/> Top Secret	<input type="checkbox"/> Secret	<input type="checkbox"/> Confidential		
d. SCIF Duty Hours	Hours to Hours:		Days Per Week:		
e. Total square footage that the SCIF occupies:					
f. Any waivers? (If Yes, attach copy of approved waiver)					<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> N/A

6. Requestor Contact Information

Name				
Phone	Open		Secure	
Email	Unclass		Classified	
Additional Email	Unclass		Classified	

7. Compartmented Area Information

a. Compartmented area accreditation level desired:				
1) Indicate CA requirements				
<input type="checkbox"/> Open Storage	<input type="checkbox"/> Closed Storage	<input type="checkbox"/> IT Processing	<input type="checkbox"/> Discussions	<input type="checkbox"/> Continuous Operation
2) Indicate the CA Type Requested (See Section C)				
<input type="checkbox"/> Type 1	<input type="checkbox"/> Type 2	<input type="checkbox"/> Type 3		

Section B: Compartmented Area Security

1. Equipment Processing

Are all equipment (computers, copiers, printers, scanners, fax, etc.) used to process compartmented information approved to process compartmented program information or a system security plan (SSP) submitted for approval to the appropriate information system authorizing official?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<i>Provide a copy of the approval documentation or a copy of the SSP submitted.</i>		

2. Workstations in a cubicle or office configuration – Type 1:

a. Is the CA in a cubicle or other open environment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Is the workstation in a closable office?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. If the office is closable, is there an access control device?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, please provide the following: MANUFACTURER _____ MODEL _____		
d. Are display screens positioned to avoid “shoulder-surfing”?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
e. Are polarized privacy screens installed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
f. Is printing of CA material required?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
If yes, explain printer location, connectivity and procedures to retrieve printed material.		

CLASSIFICATION

g. Is scanning/copying of CA material required? If yes, explain copier/scanner location, connectivity and procedures to protect CA material.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
h. Is storage of CA material required within the CA? If yes, do only individuals briefed to the CA program have access to the GSA approved storage container?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
i. Describe procedures to secure the workstation when the individual leaves the CA (for any length of time).		
j. Describe procedures to secure the CA at the end of day.		

3. CAs with a requirement for discussions of compartmented information Type 2:

a. Are all individuals within the CA briefed to the compartment? If No, describe procedures to prevent inadvertent disclosure of compartmented information.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Is the CA constructed to meet ICS 705-1 acoustic standards? If Yes, describe acoustic protection method used.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Is secure teleconferencing equipment to be used?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Describe the procedures for controlling access during program discussions and control of meeting material used (if applicable) during and after the discussions.		

4. CAs with a requirement for strict accountability of compartmented information – Type 3:

a. Are all personnel who have unescorted access to the CA briefed to the compartmented program?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
b. Does the CA meet ICS 705-1 standard for acoustic protection? (if applicable) If Yes, describe acoustic protection method used.	<input type="checkbox"/> Yes	<input type="checkbox"/> No
c. Are storage containers GSA approved?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
d. Are all equipment (computers, copiers, printers, scanners, fax, etc.) used to process compartmented information approved or a system security plan (SSP) submitted for approval?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

5. Controlling Access to Program Information

Describe the procedures for controlling access during program discussions and control of meeting material used (if applicable) during and after the discussions. In addition, include any remarks to assist in the approval process.	
--	--

6. Additional security measures (locks, alarms, dedicated reading rooms, etc.) are considers waivers (above) to the standards and require approval of the IC Element Head. Identify any additional security requirements requested:

Section C: Compartmented Area Type Descriptions

1. Compartmented Area Types

Type I: A workstation environment that is used to view and process compartmented information.

Type I comprises open bays, open spaces, or a set of rooms with multiple cubicles in an accredited SCIF where compartmented information may be securely viewed and/or processed, i.e., via an approved computer workstation by authorized personnel. Workstations in these environments may include computers with single or multiple monitors. Polarized privacy screens may be used on a computer monitor to prevent persons other than the authorized user to view the material, i.e., shoulder surfing, or when a monitor faces a primary door or common work area. In addition to processing compartmented information on approved computer workstations, Type I CAs may include the use of printers, copiers, and scanners with prior approval.

Type II: An area where discussions of compartmented information may take place. If so equipped and approved, compartmented information may also be viewed and processed.

This CA comprises a room, e.g., office or conference room, inside an accredited SCIF where compartmented discussions may be held by authorized personnel. All Type II CAs must meet existing sound transmission class (STC) requirements per ICS 705-1 to ensure that the room or office retains sound within its perimeter. In addition to compartmented discussions, Type II CAs may be used for secure video teleconferencing (SVTC) and related communication conferencing and the use of secure telephones for compartmented discussions. The use of printers, scanners, and copiers, and the secure transfer of data to approved removable media or and the use of secure facsimile machines require prior approval.

Type III: A restricted discussion area used for viewing, processing, printing, copying, storage and control of accountable compartmented information.

This CA is intended for storing and retaining compartmented information when accountability and strict control of compartmented program information is required. This includes, but is not limited to: notes, briefs, slides, electronic presentations, analytic papers, removable hard drives, field packs, thumb drives, laptops, personal electronic devices (PEDs) or hand-held devices that store compartmented information. In addition to the storage of compartmented material in a GSA-approved container, Type III CAs may be used for processing compartmented information on approved computer workstations; the use of printers, scanners, and copiers; the secure transfer of data to approved removable media; the use of secure facsimile machines; and the use of secure telephone equipment (STE) for compartmented discussions. All personnel residing within or who have unfettered access to a Type III CA must be formally briefed into all compartments that reside within the Type III CA. Visitors are permitted within Type III areas only when all compartmented information (for which the visitor is not briefed) is stored within containers, out of sight, and while the visitor is under constant observation by a fully briefed person.