

AMENDMENT OF SOLICITATION/MODIFICATION OF CONTRACT			1. CONTRACT ID CODE	PAGE OF PAGES	
			J	1	4
2. AMENDMENT/MODIFICATION NO. 0001	3. EFFECTIVE DATE 22-Jul-2003	4. REQUISITION/PURCHASE REQ. NO. W22W9K-3176-5989		5. PROJECT NO.(If applicable)	
6. ISSUED BY USA ENGINEER DISTRICT, LOUISVILLE ATTN: CELRL-CT 600 DR. MARTIN LUTHER KING PLACE ROOM 821 LOUISVILLE KY 40202	CODE DACA27	7. ADMINISTERED BY (If other than item 6) CONTRACT ADMINISTRATION BRANCH ATTN: DEBRAUH M. LARDNER P. O. BOX 59 LOUISVILLE KY 40201-0059		CODE DACA27	
8. NAME AND ADDRESS OF CONTRACTOR (No., Street, County, State and Zip Code)			X	9A. AMENDMENT OF SOLICITATION NO. DACA27-03-R-0016	
			X	9B. DATED (SEE ITEM 11) 02-Jul-2003	
				10A. MOD. OF CONTRACT/ORDER NO.	
				10B. DATED (SEE ITEM 13)	
CODE	FACILITY CODE				
11. THIS ITEM ONLY APPLIES TO AMENDMENTS OF SOLICITATIONS					
<input checked="" type="checkbox"/> The above numbered solicitation is amended as set forth in Item 14. The hour and date specified for receipt of Offer <input type="checkbox"/> is extended, <input checked="" type="checkbox"/> is not extended. Offer must acknowledge receipt of this amendment prior to the hour and date specified in the solicitation or as amended by one of the following methods: (a) By completing Items 8 and 15, and returning <u>1</u> copies of the amendment; (b) By acknowledging receipt of this amendment on each copy of the offer submitted; or (c) By separate letter or telegram which includes a reference to the solicitation and amendment numbers. FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER. If by virtue of this amendment you desire to change an offer already submitted, such change may be made by telegram or letter, provided each telegram or letter makes reference to the solicitation and this amendment, and is received prior to the opening hour and date specified.					
12. ACCOUNTING AND APPROPRIATION DATA (If required)					
13. THIS ITEM APPLIES ONLY TO MODIFICATIONS OF CONTRACTS/ORDERS. IT MODIFIES THE CONTRACT/ORDER NO. AS DESCRIBED IN ITEM 14.					
A. THIS CHANGE ORDER IS ISSUED PURSUANT TO: (Specify authority) THE CHANGES SET FORTH IN ITEM 14 ARE MADE IN THE CONTRACT ORDER NO. IN ITEM 10A.					
B. THE ABOVE NUMBERED CONTRACT/ORDER IS MODIFIED TO REFLECT THE ADMINISTRATIVE CHANGES (such as changes in paying office, appropriation date, etc.) SET FORTH IN ITEM 14, PURSUANT TO THE AUTHORITY OF FAR 43.103(B).					
C. THIS SUPPLEMENTAL AGREEMENT IS ENTERED INTO PURSUANT TO AUTHORITY OF:					
D. OTHER (Specify type of modification and authority)					
E. IMPORTANT: Contractor <input type="checkbox"/> is not, <input type="checkbox"/> is required to sign this document and return _____ copies to the issuing office.					
14. DESCRIPTION OF AMENDMENT/MODIFICATION (Organized by UCF section headings, including solicitation/contract subject matter where feasible.) Solicitation DACA27-03-R-0016 to Alter Graduate Education Facility, WPAFB, OH is hereby amended as follows: a. Changes to this solicitation are listed on the continuation pages of this amendment. b. This amendment MUST be acknowledged. c. The proposal due date remains 19 August 2003, 4:00 pm, local time.					
Except as provided herein, all terms and conditions of the document referenced in Item 9A or 10A, as heretofore changed, remains unchanged and in full force and effect.					
15A. NAME AND TITLE OF SIGNER (Type or print)			16A. NAME AND TITLE OF CONTRACTING OFFICER (Type or print)		
			TEL: _____ EMAIL: _____		
15B. CONTRACTOR/OFFEROR	15C. DATE SIGNED	16B. UNITED STATES OF AMERICA		16C. DATE SIGNED	
_____ (Signature of person authorized to sign)		BY _____ (Signature of Contracting Officer)		22-Jul-2003	

SECTION SF 30 BLOCK 14 CONTINUATION PAGE

SUMMARY OF CHANGES

SECTION SF 30 - BLOCK 14 CONTINUATION PAGE

The following have been added by full text:

AMENDMENT 00001

d. The following are the changes made by this amendment:

1. Drawings and specifications for the Sensitive Compartmented Information Facility (SCIF)

Specification sections -

Table of Contents

02084	PCB Spill Cleanup & Site Restoration
03350	Concrete Repair
04250	Masonry Repair
05055	Welding, Structural
07213	Fibrous Batt Insulation
08700	Hardware
11132	Projection Screens
15951A-1	Addition to Direct Digital Control for HVAC for SCIF
16198B	Directories for Existing Panel boards
16730A	Intrusion Detection System

Drawings -

A001

A101

A201

E101

E102

F101

M101

M401

M601

2. Add the document DCID 1/21, Director of Central Intelligence Directive 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIF).

3. Specification Section 00800, add paragraph 1.6 Exclusion of Periods in Computing Completion of Schedules, "No work will be required during the period between NTP and 80 calendar days after issue of the NTP inclusive, and such period has not been considered in computing the time allowed for completion. The Contractor may, however, perform work during

all or any part of this period upon giving prior written notice to and receiving approval from the Contracting Officer."

4. NOT USED

5. Delete note for site visit, 52.236-27 (c), replace with, Submit all names of expected site visit participants to Ken Stegall, 937-255-2967, by 4 pm (local time), 23 July 2003. Participants will meet at Building 20640, Wright-Patterson AFB, 29 July 2003 at 10:00 AM, for the site visit.

6. Phase 1 of the project is in the high bay area of the building and is defined in the plans as the area within column lines 12-16, and A-H on all three floors. Phase 1 must be completed within 360 calendar days and prior to completion of Phase 2, which is the balance of the construction contract.

DRAWINGS

7. Sheet C1.0: Change Layout Keynote 7 to read, "Concrete curb and sidewalk. See detail this sheet"; change layout Keynote 2 to read, "Concrete sidewalk. Match existing grade at each end. See taper curb and ramp detail this sheet."

8. Sheet C2.1: Change Keynote 5 to read, "Not Used". On "Site Plan – Grading and Drainage", remove keynote 5 and related piping for sump shown at northwest corner of proposed stair/elevator addition.

9. Sheet A11.6: Detail 9/A11.6, add Keynote 17 to denote the architectural pre-cast concrete unit immediately below the sill of the aluminum entrance and storefront system.

10. NOT USED

11. Sheet A14.3: Enlarged Plan 10/A14.3, change the referenced room number to "253".

12. Sheet T1.0: "Extend line from Keynote 1 to the bold dashed line encircling rooms 108, 108B, 108C, 108D, 108E, 108F, 108G, 108H, 108J, 108K 108L and 108M. Change the room reference in Keynote 1 to read "108A

13. Sheets T1.0, T1.1A, T1.1B and T1.2a : In the Legend, add a small "R" to the second triangle symbol to denote "Mounted in 1" surface raceway with surface mounted box"

14. Sheet AD.0: In Demolition Environmental Notes, add "assume all previously painted surfaces to contain lead" to Note 7.

15. Sheet A5.0: Replace with updated sheet issued with this amendment. Roof mounted AHU's have been shown. Room No. 300 "Penthouse" has been changed to Room No. 400. Change General Note D to read, "Remove and replace existing lightning protection system. See Sheet E2.3."

16. Sheet M1.1B: replace with updated sheet issued with this amendment. Air supply to SCIF area has been revised to coordinate with SCIF drawings.

17. Sheet M1.2B: Replace with updated sheet issued with this amendment. Piping to SCIF area has been revised to coordinate with SCIF drawings.

18. Sheet M3.1: Add FD-1 in supply ducts from AHU-1,2 & 3 as shown on M1.0.

19. Sheet SP1.2A: Change title of Mezzanine Floor Plan.... to Penthouse Floor Plan....

SPECIFICATIONS

20. Section 01451: In paragraph 3.4.3, item g, delete the requirements and insert "not used".

21. Submittal Register: Add required submittals for Sections 01020, 01451L, 02081, 02083C, 02083D, 02090, 02091, 08346, 10550, and 16750 to the register as indicated in the attached supplement.

22. Section 07900: Paragraph 2.4.2, b - add the following to Applications, "Include joints between concrete or masonry and mechanical or electrical items penetrating exterior walls."

23. Section 15895: Page 23, Paragraph 2.10.2 change heading for paragraph to "Factory Fabricated Air Handling Units Including Rooftop Units".

24. Section 15895: Page 24, Paragraph 2.10.2.1 add to end of paragraph "Rooftop unit construction shall be watertight with sloping roof for drainage."

25. Section 15895: Page 26, add Paragraph, "2.10.2.8 Roof Curb: Provide factory constructed roof curbs as supplied by the rooftop unit manufacturer. Provide curbs 12 inches in height with top of curb level."

26. Section 15895: Page 26, add Paragraph, "2.10.2.9 Other Unit Components: See equipment schedule for other components. Provide manufacturer's standard components when applicable."

27. Section 15995A: Pages 234, 237, 239, 241, 243, 245, 247, 249, 251, 253 and 254, add "Design Agent Representative" to list of certification team participants.

28. Section 15951A: Page 2, Paragraph 1.2, change 2nd and 3rd sentences to: "Provide system manufactured by Johnson controls, Staefa or equal. Connect system to the base EMCS system by Ethernet Communication cable . Provide system 100% compatible with the Staefa/Johnson control systems.

29. Section 15895: Page 17, add paragraph: "2.8.3.4 Combination Fire/Smoke Dampers: Label according to UL 555S. Combination fire and smoke dampers shall be labeled according to UL 555 for 1-1/2 rating. Fusible links shall be electronic "resettable" fuse line, UL classified with reset and test switch. Frame and blades shall be minimum 0.064-inch thick, galvanized

sheet steel or 14 gauge equivalent air foil shape. Mounting sleeve shall be factory-installed, 0.052-inch thick, galvanized sheet steel; length to suit wall or floor application. Damper motors shall be modulating and two position action. Motors shall be permanent-split-capacitor or shaded-pole motors with oil-immersed and sealed gear trains. Motors shall have spring returns equipped with integral spiral-spring mechanism designed for slow closing. Enclose entire spring mechanism in a removable housing designed for service or adjustments. Size for running torque rating of 150 in.x lbf and breakaway torque rating of 150 in.x lbf. Outdoor motors and motors in outside air intakes shall be equipped with O-ring gaskets designed to make motors weatherproof. Equip motors with internal heaters to permit normal operation at minus 40 deg f. When smoke is detected, during testing or if power failure occurs, the damper will close and remain closed. when the smoke signal ceases, the test is completed or power is restored the damper will automatically reset to the open position. The damper shall automatically reset if nuisance alarms occur and the system is reset. When temperatures in excess of 165 rF are detected, the damper will close and lock. Upon cessation of the fire conditions, the damper can be reopened by pressing the reset button located on the damper assembly. Electrical power shall be 115 volts, single phase, 60 HZ.”

30. Section 16750: Paragraph 2.6.5, change heading to read, “25-Pair Cable Unshielded Twisted Pair - CMP”.

31. Section 16750: Paragraph 3.4.1.4, j; change the first sentence of both subparagraphs 7 and 8 to read, “Provide 48 strand multi-mode, 36 strand single mode optical fiber cables from ...”

32. Section 16750: Paragraph 3.4.1.4, j; subparagraph 9; change heading to read, “Facility 20640 to Facility 20644 (Route 1)”.

33. Section 16750: Paragraph 3.4.1.4, j, subparagraph 10; change heading to read, “Facility 20640 to Facility 20644 (Route 2)”.

(End of Summary of Changes)

SECTION 02084

PCB SPILL CLEANUP AND SITE RESTORATION

PART 1 - GENERAL

1.01 SECTION INCLUDES

- A. Remove and/or decontaminate all concrete, soils and/or surfaces contaminated with an existing Polychlorinated Biphenyl (PCB) spill as indicated on the drawings. Verify successful cleanup of all PCB spills and restore the site to conditions found before decontamination (i.e., pour concrete, fix walls, etc.)
- B. Containerize all contaminated liquids, debris, and disposable equipment generated during the cleanup of all existing PCB spills. Prepare and transport all containerized material to the Defense Reutilization and Marketing Office (DRMO), Bldg 743, Area B, Wright-Patterson Air Force Base. Ownership of PCB spill and cleanup materials shall remain with the Government.

1.02 REFERENCES

- A. Environmental Protection Agency, EPA:
 - 1. Title 40 Code of Federal Regulations, Part 761; Subpart G - PCB Spill Cleanup Policy.
 - 2. Title 40 Code of Federal Regulations, Part 761, 261, 262, 263; all applicable Subparts, most recent amendment.
- B. Occupational Safety and Health Administration, OSHA:
 - 1. Title 29 Code of Federal Regulations, Part 1910 and Part 1926; all applicable subparts, most recent amendment (especially 1910.120).
- C. Department of Transportation, DOT:
 - 1. Title 49 Code of Federal Regulations, Part 171, 172, 173, 177 and other applicable parts, most recent amendment.
- D. Other Applicable References
 - 1. EPA-560/5-86-014, "Field Manual for Grid Sampling of PCB Spill Sites to Verify Cleanup".
 - 2. EPA Methods 608 and 8080, "Organochlorine Pesticides and PCBs".
 - 3. ANSI/ASTM D 3304-77, "Analysis of Environmental Materials for Polychlorinated Biphenyl (PCB)".

1.03 SPILLS

- A. Immediately report new or newly discovered existing PCB spills of any size to Environmental Management, 257-7455, Contract Management, 257-2047 and Civil Engineering Service Call, 257-6764.

1.04 SUBMITTALS

- A. Submit a Project Work Plan for approval. This plan shall include the following:

NOTE: SUBMITTAL INFORMATION REQUESTED IN LINES 1,2,3 AND 5 BELOW IS NOT REQUIRED IF THE INFORMATION IS ALREADY BEING SUBMITTED FOR APPROVAL IN ACCORDANCE WITH SECTION 02083.

1. Detailed procedures for the removal and handling of PCB and PCB contaminated items and liquids in compliance with all applicable regulations.
 2. A Health and Safety Plan satisfying the criteria of 29 CFR 1910.120.
 3. A Spill Prevention, Countermeasures and Control Plan including a Transportation and Containment Plan (40 CFR 264.50, 49 CFR, and 29 CFR 1910.120).
 4. A Quality Assurance Project Plan including procedures for obtaining verification samples, prevention of cross-contamination, chain-of-custody procedures and analysis.
 5. A detailed project schedule indicating the sequence of operations to be performed.
- B. Provide PCB spill cleanup reports within 10 working days upon completion of cleanup at each site.
1. Site specific PCB spill reports shall be as defined in Subpart G, 40 CFR 761. Include analytical results, chain-of-custody records, sampling strategy, etc.

1.05 COORDINATION

- A. Contractor shall notify the following in writing at least ten (10) working days prior to initiating cleanup of an existing PCB spill.
1. 645 CEG/CECC Contract Management (Project Inspector).
 2. 645 ABW/EMC Environmental Management (Waste Management).
- B. The names of the personnel to be notified will be given to the contractor at the pre-construction meeting.

1.06 PROTECTIVE EQUIPMENT

- A. The contractor shall provide and maintain all personal protective equipment required by 29 CFR 1910 to perform PCB spill cleanup operations. This equipment is to be disposable to the extent allowable by regulation.
1. Protective equipment shall include, among other things; gloves, coveralls, boots, and cartridge respirators.

1.07 DEFINITIONS

- A. POLYCHLORINATED BIPHENYL (PCB): Any chemical substance that is limited to the biphenyl molecule that has been chlorinated to varying degrees or any combination of substances which contains such substance.
- B. PCB SPILL: The intentional and/or unintentional spills, leaks, and other uncontrolled discharges where the release results in any quantity of PCB, running off or about to run off the external surface of the equipment; and the contamination resulting from those releases.
- C. LOW CONCENTRATION PCB SPILL: Spills from equipment that has been tested and found to contain PCBs greater than 50 ppm but less than 499 ppm prior to the spill or those which the EPA

requires to be assumed between 50 and 499 ppm. These spills involve less than 1 pound of PCB by weight.

- D. HIGH CONCENTRATION PCB SPILL: Spills from equipment that has been tested and found to contain PCBs greater than 500 ppm prior to the spill or those which the EPA requires to be assumed at 500 ppm or above. Includes those spills of low concentration PCB involving greater than 1 pound of PCB by weight.

1.08 PERFORMANCE REQUIREMENTS

- A. The cleanup standards defined in 40 CFR 761; Subpart G, PCB spill cleanup policy shall be met and certified complete by the contractor in compliance with all applicable sections of this EPA policy.

1.09 QUALIFICATIONS

- A. The analytical laboratory used for analysis of samples of various media for PCBs shall report the results of swipe samples in micrograms per 100 square centimeters. Soils and other media sample results are to be reported in mg/kg. Analytical results must be attainable within 48 hours.

PART 2 - PRODUCTS

Not Used

PART 3 - EXECUTION

3.01 SECURITY OF SITES

- A. Install self-supporting barricades and post PCB spill warning signs. Establish a single entrance to the site.

3.02 SPILL CONTAINMENT

- A. Provide six mil plastic drop cloths or metallic drip pans where spillage may occur.
- B. Secure all floor drains, conduits and other openings.
- C. Use absorbent material to prevent contaminant migration under existing devices.

3.03 EQUIPMENT DECONTAMINATION

- A. Decontaminate all nondisposable items contaminated with PCB during the cleanup prior to exiting each site. Wipe all contaminated solid surfaces a minimum of three times with an organic solvent and swipe. Do not reuse the swipe. Capture all runoff. Do not reuse the contaminated solvent.
- B. Contain contaminated materials in DOT approved drums.

3.04 CLEANUP OF ALL LOW CONCENTRATION EXISTING PCB SPILLS ON CONCRETE SURFACES AND IN ACCESSIBLE SOILS

- A. Ensure Environmental Management (EM) representatives are on-site prior to starting cleanup.
- B. Establish spill boundaries per contract drawings and visible evidence of dielectric oil stains. PCB stains are to be covered with six mil plastic sheeting prior to mobilization.
- C. Install self-supporting barricades and post PCB spill warning signs. Establish a single entrance.
- D. Secure all floor drains, conduits and other openings.

- E. Use absorbent material to prevent contaminant migration under existing devices.
- F. Decontaminate all solid surfaces through a double-rinse wash. Cleanup of PCB will be done with a commercial/industrial liquid cleaner containing limonene as the organic solvent and an emulsifier. Apply with a portable sprayer, scrub the affected surfaces and rinse with clean water. Concurrently capture all free-flowing liquids using a wet vacuum. Repeat the decontamination process until all visible evidence plus a three foot buffer zone has been completed.
- G. Remove all soils within the spill area (i.e., visible traces of contaminated soil and a buffer zone of one lateral foot around the visible traces) using portable hand tools. Excavate to a minimum depth of ten inches. Backfill with clean noncontaminated soil.

3.05 CLEANUP OF HIGH CONCENTRATION EXISTING PCB SPILLS ON CONCRETE SURFACES

- A. Implement the requirements outlined in paragraph 3.04 (A) through (E).
- B. Remove all PCB stains via cloth wipe and an organic solvent. Use absorbent pads to control all liquid runoff.
- C. Scarify the concrete pad surfaces to a depth of 1/4 inch. Concrete floors and foundations are to be scarified to a depth of 1/8 inch where noted on the drawings. Use a concrete scarifier with an High Efficiency Particulate Air (HEPA)-filtered vacuum exhaust system to concurrently capture all contaminated dust generated.
- D. Decontaminate scarified concrete surfaces using the double-rinse wash procedures outlined in paragraph 3.04.F. Allow the entire floor area to dry.
- E. Conduct post cleanup grid verification sampling in accordance with EPA-560/5-86-014. Composite sampling is not allowed. Await receipt of verification samples and coordinate with EM on cleanup results prior to performing site restoration.

3.06 CLEANUP OF LOW AND HIGH CONCENTRATION EXISTING PCB SPILLS EXTENDING INTO EXPANSION JOINTS AND CRACKS

- A. Implement the requirements outlined in 3.04 paragraph (A) through (C).
- B. Implement concrete scarification and/or selective demolition to a maximum depth of 1/2 inch. Control and collect all dust generated through the use of an HEPA-filtered vacuum exhaust system. If visible evidence remains, contact the Contracting Officer for further instructions.
- C. Conduct post cleanup verification sampling in accordance with EPA-560/5-86-014. Composite sampling is not allowed. Await receipt of verification samples and coordinate with EM on cleanup results prior to performing site restoration.

3.07 PCB SPILL WASTE CONTAINERIZATION

- A. Contain all solid PCB-contaminated material (soil, concrete, disposable clothing, etc.) in 30 or 55-gallon open head steel shipping drums. The drums shall meet DOT 17C specifications and must be in good condition. Do not mix liquids with solid materials.
- B. Contain all liquids in 30 or 55-gallon closed head steel shipping drums. The drums shall meet DOT 17E specifications and must be in good condition. Do not fill over 90% of the drum capacity.

3.08 CONTAINER MARKING

- A. Durably mark all containers according to the PCB concentration of the dielectric oil spilled, not the concentration of PCB in the material removed. Use the appropriate PCB label per Figure 1, 2, 3 or 4.
- B. Durably mark all containers with the date they are sealed and placed in temporary storage.

3.09 TEMPORARY STORAGE

- A. Coordinate the temporary storage location (for PCB and PCB contaminated items) with the Contracting Officer.
- B. Individually date all items to show when the drum was filled and placed in temporary storage.
- C. Do not have any item in temporary storage for over 30 calendar days. Do not relocate items for the purpose of extending the storage time.
- D. Place drip pans or six mil plastic sheeting under equipment to prevent possible seepage into the ground. Protect containers from rainwater.

3.10 DOCUMENTATION FOR TURN-IN

- A. Environmental Management Assistance. Contact Environmental Management (EM), Room 129, Building 89, Area C, for assistance with obtaining turn-in documents and coordinating DRMO turn-in at least five (5) working days prior to working at a site. The name of the person to contact will be provided at the pre-performance meeting. Be prepared to provide the following information on each piece of equipment:
 - 1. Serial number, manufacturer, date of manufacture (if available), voltage, kVA, oil capacity, dimensions, weight, PCB concentration of each piece of equipment or the specific contents, and the estimated weight and quantity of drums. EM will prepare an AF Form 2005 for each item.
- B. EM Certification. EM will conduct a site inspection required for certification of items to be turned in. EM will provide an AFLC Form 165, Hazardous Waste Label, to be applied to each item prior to turn-in.
- C. Document Processing. EM will process the AF Form 2005 and prepare a DD Form 1348-1. Allow two (2) working days for processing the forms. Contact EM to obtain the completed 1348-1 turn-in document.
- D. Turn-in Scheduling. When the DD Form 1348-1 is picked up by the Contractor, EM will coordinate a turn-in date and time with DRMO for the Contractor. Immediately contact EM if the scheduled time cannot be met.
- E. Hazardous Waste Manifest. An EPA Uniform Hazardous Waste Manifest is required when transporting more than one (1) pound of PCBs on a public highway that is outside the Wright-Patterson reservation boundary. Coordinate a date and time for an EM representative to sign the manifest prior to transporting.
- F. Packing List. Prepare a document for each PCB item that contains the information requirements in paragraph 3.04.A.1. The document shall be 8-1/2" by 11" size and either typewritten or legibly hand written. Affix one copy to the PCB item and furnish one copy to the DRMO at the time the PCB items are delivered.

3.11 TRANSPORT

- A. Provide pallets for all items that are to be forklifted and secure these items to pallet with metal banding.
- B. Utilize a trucking firm that has a USEPA identification number and is licensed in the State of Ohio for transporting hazardous material if the load contains over one pound of PCBs and the route taken includes a public highway that is outside the Wright-Patterson AFB reservation boundary.
- C. The Contractor turn-in to DRMO shall be between 0830 and 1500 hours during the weekdays.
- D. Unload and move into storage all items in accordance with DRMO instructions. Provide all equipment required (forklift, dolly, etc.).

3.12 LABELING

- A. Label (as shown in Figure 1, 2, 3, or 4) all equipment, drums, etc. according to the PCB concentration of the oil, material contained or the oil removed from the item. Affix the label prior to working on or utilizing the item. The following formats shall be used for labeling:
1. PCB Items or containers containing PCBs equal to or greater than 500 ppm.
 - (a) Large PCB Mark--ML. Mark ML shall be as shown in Figure 1, letters and striping shall be on a white or yellow background and shall be sufficiently durable to equal or exceed the life (including storage for disposal) of the PCB Article, PCB Equipment, or PCB Container. The size of the mark shall be at least 15.25 cm (6 inches) on each side. If the PCB Article or PCB Equipment is too small to accommodate this size, the mark may be reduced in size proportionately down to a minimum of 5 cm (2 inches) on each side.
 - (b) Small PCB Mark--Ms. Mark Ms shall be as shown in Figure 2, letters and striping on a white or yellow background and shall be sufficiently durable to equal or exceed the life (including storage for disposal) of the PCB Article, PCB Equipment, or PCB Container. The mark shall be a rectangle 2.5 by 5 cm (1 inch by 2 inches). If the PCB Article or PCB Equipment is too small to accommodate this size, the mark may be reduced in size proportionately down to a minimum of 1 by 2 cm (0.4 by 0.8 inches).
 2. PCB Contaminated Items or Containers containing PCBs in concentrations between 50 and 499 ppm.
 - (a) PCB Contaminated Mark. Mark shall be as shown in Figure 3, letters and striping on a white or yellow background and shall be sufficiently durable to equal or exceed the life (including storage for disposal) of the PCB Contaminated Article, PCB Contaminated Equipment, or Container of PCB Contaminated oil. The mark shall be a rectangle 10 by 10 cm (4 inch by 4 inches). If the PCB Contaminated Article or PCB Contaminated Equipment is too small to accommodate this size, the mark may be reduced in size proportionately down to a minimum of 5 by 5 cm (2 by 2 inches).
 3. Non-PCB Items containing PCB in concentrations equal to or less than 49 ppm.
 - (a) Non-PCB Mark This mark shall be as shown in Figure 4, letters and striping on a blue background and shall be sufficiently durable to exceed the time the Non-PCB Article, Equipment, or Container is stored on Wright-Patterson Air Force Base.

```
////////////////////////////////////  
/          CAUTION          /  
/          contains        /  
/          PCBs            /  
/          (Polychlorinated Biphenyls) /  
/ A toxic environmental contaminant requiring /  
/ special handling and disposal in accordance with /  
/ U.S. Environmental Protection Agency Regulations /  
/ 40 CFR 761 - For Disposal Information contact /  
/ the nearest U.S. E.P.A. Office. /  
/ ***** /  
/ /  
/ In case of accident or spill, call toll free the U.S./  
/ Coast Guard National Response Center /  
/ 1-800-424-8802 /  
/ /  
/ Also Contact /  
/ Tel. No. /  
////////////////////////////////////
```

Figure 1

```
////////////////////////////////////  
/ CAUTION contains PCBs /  
/ (Polychlorinated Biphenyls) /  
/ /  
/ FOR PROPER DISPOSAL INFORMATION /  
/ CONTACT U.S. ENVIRONMENTAL /  
/ PROTECTION AGENCY /  
////////////////////////////////////
```

Figure 2

```
////////////////////////////////////  
/                               /  
/   PCB CONTAMINATED         /  
/                               /  
/   THE LIQUID IN THIS       /  
/   CONTAINER IS LESS        /  
/   THAN 500 PPM PCB         /  
/   BUT EQUAL TO             /  
/   OR GREATER THAN          /  
/   50 PPM PCB               /  
/                               /  
////////////////////////////////////
```

Figure 3

```
//////////  
/         /  
/ NO PCBs /  
/         /  
//////////
```

Figure 4

END OF SECTION

SECTION 03350

CONCRETE REPAIR

PART 1 - GENERAL

1.01 WORK INCLUDED:

- A. Temporary shoring and protection of existing materials and equipment.
- B. Restoration of areas damaged during the course of this work.

1.02 APPLICABLE PUBLICATIONS: THE PUBLICATIONS LISTED BELOW FORM A PART OF THIS specification to the extent referenced. The publications are referenced in the text by the basic designation only.

- A. American Concrete Institute (ACI)
 - ACI 318 Building Code Requirements for Reinforced Concrete
- B. U.S. Army Corps of Engineers Handbook for Concrete and Cement:
 - CRD-C 104 Calculation of the Fineness Modulus of Aggregate
 - CRD-C 300 Membrane-Forming Compounds for Curing Concrete
 - CRD-C 400 Water for Use in Mixing or Curing Concrete
- C. American Society for Testing and Materials (ASTM) :
 - A 185 Welded Steel Wire Fabric for Concrete Reinforcement
 - A 615 Deformed and Plain Billet Steel Bars for Concrete Reinforcement Grade 60
 - C 31 Making and Curing Concrete Test Specimens in the Field
 - C 94 Ready-Mixed Concrete
 - C 125 Standard Terminology Relating to Concrete and Concrete Aggregates
 - C 136 Sieve Analysis of Fine and Coarse Aggregates
 - C 143 Slump of Portland Cement Concrete
 - C 150 Portland Cement
 - C 171 Sheet Materials for Curing Concrete
 - C 173 Air Content of Freshly Mixed Concrete by the Volumetric Method
 - C 192 Making and Curing Concrete Test Specimens in the Laboratory
 - C 231 Air Content of Freshly Mixed Concrete by the Pressure Method
 - C 260 Air-Entraining Admixtures for Concrete

C 309	Liquid Membrane-Forming Compounds for Curing Concrete
C 881	Epoxy-Resin-Base Bonding Systems for Concrete
D 75	Sampling Aggregates

1.03 DESIGN: THE CONCRETE MIXTURES SHALL BE DESIGNED TO PRODUCE CONCRETE HAVING AN average flexural strength of 700 psi at 7 days of age, determined in conformance with ASTM C 78, using standard 6- by 6-inch beam specimens. The concrete mixtures shall be designed to secure an air content by volume of 6 percent, plus or minus 1-1/2 percent, based on measurements made on concrete immediately after discharge from the mixer in conformance with ASTM C 231. The slump of the concrete mixture shall not exceed 2" when tested in accordance with ASTM C 143.

1.04 SAMPLING AND TESTING OF MATERIALS: SAMPLING AND TESTING SHALL BE PERFORMED BY an approved commercial laboratory. The first laboratory inspection, if requested by the Government, shall be at the expense of the Government and the cost of any subsequent inspection resulting from failure of the first inspection shall be at the expense of the Contractor. Such costs shall be deducted from the total amount due to the Contractor. All testing shall be performed at no additional cost to the Government.

- A. Cement: Cement shall be tested as prescribed in the referenced specification under which it is furnished. Cement may be accepted on the basis of mill tests and the manufacturer's certification of compliance with the specification, provided the cement is the product of a mill with a record for the production of high-quality cement for the past 3 years.
- B. Aggregate: Aggregate samples for laboratory testing shall be taken in conformance with ASTM D 75 and tested in accordance with ASTM C 136.
- C. Epoxy-Resin Grout: Epoxy-resin grout shall be tested for conformance with ASTM C 881.
- D. Samples for Mixture Proportioning: Mix design studies and tests shall be made in accordance with ASTM C 78 and C 192, and the test results submitted for approval.

1.05 SUBMITTALS

A. CONCRETE

- 1. Job-Mix-Formula: The Contractor shall develop and submit a proposed mix design prior to placement. The mix design shall indicate the weight of each ingredient of the mixture. No concrete shall be placed prior to approval of the proposed mix design. No deviation from the approved job-mix formula will be permitted without prior approval.
- 2. Laboratory Test Results: Within 48 hours of physical completion of laboratory testing, 5 copies of test results shall be submitted for approval.
- 3. Certification: Manufacturer's certifications may be submitted rather than laboratory test results for proposed materials. Certificates should certify compliance with the appropriate specification referenced herein. No materials shall be placed without prior approval from the Contracting Officer.

B. CURING MATERIALS

- 1. Product Data.
- 2. Curing method plan defining proposed curing procedures.

C. EPOXY RESIN GROUT

1. Product data.
2. Letter of certification.

1.06 DELIVERY AND STORAGE OF MATERIALS:

- A. Cement: Cement may be furnished in bulk or in suitable bags used for packaging cements and shall be stored in a manner to prevent absorption of moisture.
- B. Aggregates: Aggregates shall be handled and stored in a manner to avoid breakage, segregation, or contamination by foreign materials.
- C. Epoxy-Resin Grout: Epoxy-resin grout shall be delivered to the site in such manner as to avoid damage or loss. Storage areas shall be in a weatherproof, but ventilated, insulated building, with provision for conditioning the material to 70 degrees F to 85 degrees F for a period of 48 hours prior to use. The ambient temperature in the storage area of the epoxy materials shall at no time be higher than 100 degrees F.

PART 2 - PRODUCTS

2.01 BASIC MATERIALS

A. Coarse Aggregate:

1. Composition: Coarse aggregate shall consist of crushed gravel, crushed stone, or a combination thereof, or crushed blast-furnace slag. Crushed gravel, according to ASTM C 125, shall be the product resulting from the artificial crushing of gravel with substantially all fragments having at least one face resulting from fracture.
2. Quality: Aggregate as delivered to the mixers shall consist of clean, hard, unweathered, and uncoated particles. Dust and other coatings shall be removed from the coarse aggregates by adequate washing.
3. Particle Shape: Particles of the coarse aggregate shall be generally spherical or cubical in shape.
4. Size and Grading: The maximum nominal size of the coarse aggregate shall be 3/8-inch. The coarse aggregate shall be well graded within the limits specified, and when tested in accordance with ASTM C 136, shall conform to the following grading requirements as delivered to the batching hoppers:

Sieve Size	Percentage by weight, passing
1/2 inch	100
3/8 inch	85-100
No. 4	10-30
No. 8	0-10
NO. 16	0-5

B. Fine Aggregate:

1. Composition: Fine aggregate shall consist of either natural sand, manufactured sand, or a combination of natural and manufactured sand, and shall be composed of clean, hard, durable particles.
2. Particle Shape: Particles of the fine aggregate shall be generally spherical or cubical in shape.
3. Grading: Grading of the fine aggregate as delivered to the mixer shall conform to the following requirements when tested in accordance with ASTM C 136.

Sieve Size	Percentage by weight, passing
3/8 inch	100
No. 4	95-100
No. 8	80-90
No. 16	60-80
No. 30	30-60
No. 50	12-30
No. 100	2-10

In addition, the fine aggregate, as delivered to the mixer, shall have a fineness modulus of not less than 2.40 nor more than 2.90, when calculated in accordance with Corps of Engineers Specification CRD-C 104.

- C. Air-Entraining Admixture: Air-entraining admixture shall conform to ASTM C 260.
- D. Cement: Cement shall be portland cement conforming to ASTM C 150, Type I or Type III.

2.02 CURING MATERIALS

- A. Burlap shall conform to Fed. Spec. CCC-C-467, class 4.
- B. Membrane-forming curing compound shall be a pigmented type conforming to Corps of Engineers Specification CRD-C 300.
- C. Waterproof blanket materials shall conform to ASTM C 171, Type optional, color white.

2.03 EPOXY-RESIN GROUT

- A. Epoxy-resin grout shall be a two-component, epoxy-resin bonding system for application to portland-cement concrete, which is able to cure under humid conditions and bond to damp surfaces.
- B. The epoxy-resin grout shall conform to ASTM C 881, Type V. Class B material shall be used when the existing surface temperature is between 40 and 60 degrees F. Class C material shall be used when the existing surface temperature is above 60 degrees F.

2.04 EPOXY PATCHING MATERIAL (MINOR AREAS)

- A. Concrete Bonding Agent; Sonneborn "Sonobond"; two-component, 100% epoxy resin, adhesive system.
- B. Concrete Patching Material; Sonneborn "Epolith Patcher", two component, aggregate filled, epoxy resin patching compound.

2.05 WATER

- A. Water shall be clean, fresh, and free from injurious amounts of oil, acid, salt, alkali, organic matter, or other deleterious substances. Water approved by Public Health authorities for domestic consumption may be accepted for use without being tested. Water that is of questionable quality, in the opinion of the Contracting Officer shall be tested in accordance with CRD-C 400.

PART 3 - EXECUTION

3.01 CONDITIONING OF EXISTING SURFACES

- A. Preparation of Existing Surfaces: In the area to be patched, the surface of the existing concrete shall be removed to a minimum depth of one inch and to such additional depth where necessary to expose a surface of sound, unweathered concrete that is uncontaminated by oils, greases, salts or solutions. A vertical saw cut at least one inch deep shall be made a minimum of one inch outside of the area to be repaired. The surface shall be thoroughly cleaned by sweeping and blowing with compressed air. Prior to coating with the epoxy-resin grout, areas showing traces of oils or grease shall be cleaned by sandblasting.
- B. Bonding Course: Prior to placing concrete, the previously prepared surfaces shall be washed with a high pressure water jet followed by an air jet to remove free water. The clean surface shall then be coated with a 20- to 40- mil thick film of the epoxy-resin grout. The epoxy-resin grout shall be placed in one application, just prior to concrete placement, with the use of mechanical combination, mixing and spraying equipment, or shall be applied in two coats with stiff brushes. The first brush coat shall be scrubbed into the concrete surface, followed by an additional brush coat to obtain the required thickness. When the brush method is used, the initial coat may be allowed to dry; however, the final coat shall be applied just prior to placement of the concrete.
 - 1. Epoxy-resin grout components shall be mixed in the proportions recommended by the manufacturer. The components shall be conditioned to 70 degrees F to 85 degrees F for 48 hours prior to mixing. The two epoxy components shall be mixed with a power-driven, explosion proof stirring device in a metal or polyethylene container having a hemispherical bottom. The curing-agent component shall be added gradually to the epoxy-resin component with constant stirring until a uniform mixture is obtained. The rate of stirring shall be such that the entrained air is a minimum.
 - 2. Tools and equipment used further in the work shall be thoroughly cleaned before the epoxy-resin grout sets.
 - 3. The following health and safety precautions shall be followed:
 - a. Full face shields shall be provided for all mixing and blending operations and for placing operations as required.
 - b. Protective coveralls and neoprene-coated gloves shall be provided for all workmen engaged in the operations.
 - c. Protective creams of a suitable nature for the operation shall be supplied.
 - d. Adequate fire protection shall be maintained at all mixing and placing operations.
 - e. Smoking or the use of spark or flame-producing devices shall be prohibited within 50 feet of mixing and placing operations.

- f. The mixing, placing, or storage of epoxy-resin grout or solvent shall be prohibited within 50 feet of any vehicle, equipment, aircraft, or machinery that could be damaged from fire or could ignite vapors from the material.

3.02 BATCHING, MIXING AND PROPORTIONING

- A. Equipment: The batching and mixing plant may be located off base. The Contractor shall provide adequate facilities for the accurate measurement and control of each of the materials entering the concrete. The Contracting Officer shall have free access to the batching and mixing plant at all times. Mixing equipment shall be capable of combining the aggregate, cement, admixture, and water into a uniform mixture and discharging this mixture without segregation.
- B. Conveying: Concrete shall be conveyed from mixer to repair area as rapidly as practicable by methods that will prevent segregation or loss of ingredients.
- C. Mix Proportions: The proportions of materials entering into the concrete mixtures shall be in accordance with the approved job-mix formula. The proportions shall be changed whenever necessary to maintain the workability, strength, and standard of quality required, and to meet the varying conditions encountered during the construction. However, no changes will be made without prior approval.
- D. Measurement: Equipment necessary to measure and control the amount of each material in each batch of concrete shall be provided. Bulk cement shall be weighed, but cement in unopened bags as packed by the manufacturer may be used without weighing. If bagged cement is used, batches shall be proportioned so that fractional bags will not be required. One bag of portland cement will be considered as weighing 94 pounds. Mixing water and air-entraining admixtures may be measured by volume or by weight. One gallon of water will be considered as weighing 8.33 pounds.
- E. Workability: The slump of the concrete shall be maintained at the lowest practicable value, not exceeding 2 inches when tested in accordance with ASTM C 143.

3.03 FORMS

- A. Provide formwork as required to duplicate the concrete contours and shapes of the existing structure. The forms and associated false work shall be substantial and unyielding and shall be constructed so that the finished concrete will conform to the specified dimensions and contours with no deviation greater than 1/4 inch. Form surfaces shall be smooth and free from holes, dents, sags or other irregularities. Forms shall be coated with nonstaining form oil before being set into place. Metal ties or anchorages within the forms shall be equipped with cones, she-bolts or other devices that permit their removal to a depth of at least one inch without injury to the concrete. Ties designed to break off below the surface of the concrete shall not be used without cones.

3.04 PLACING

- A. Concrete shall be placed within 45 minutes from the time all ingredients are charged into the mixing drum, before the concrete has obtained its initial set, and while the epoxy-resin bonding course is tacky.
- B. The temperature of the concrete, as deposited in the form, shall be not less than 40 degrees F nor more than 90 degrees F.
- C. Concrete shall be deposited in such manner as to require a minimum of rehandling, and the placement shall be in such manner so as to least disturb the epoxy-resin grout. The placing of concrete shall be rapid and continuous for each area.

- D. The concrete shall be thoroughly consolidated by tamping or by means of suitable vibrating equipment.
- E. Prior to placement of concrete the forms shall be free of debris, ice, snow, extraneous oil, or other harmful substances or coatings. Any oil on the reinforcing steel or other surfaces required to be bonded to the concrete shall be removed.
- F. Items to be embedded in the concrete shall be positioned accurately before placing concrete and held securely in position.
- G. Bars or heavy tools shall not be used against the concrete in removing the forms. Any concrete damaged in form removal shall be repaired promptly by the contractor at no cost to the Government.
- I. After removal of forms, formed surfaces shall be patched as follows: Remove loose material, cut back unsound concrete, voids over 1/2 inch diameter, and tie rod and bolt holes to sound concrete; fill holes with a stiff portland cement mortar mix. Make patching mortar using some white cement with the regular cement and sand. Mix patching mortar to match surrounding concrete.
- J. Expansion and control joints shall be provided where ever located in the existing structure.

3.05 FIELD TEST SPECIMENS:

- A. General: Concrete samples shall be taken in the field and tested by the contractor to determine the slump. The slump shall be determined in conformance with ASTM C 143 twice each day.

3.06 FINISHING CONCRETE

- A. General: Repair areas shall finish flush with adjoining concrete surfaces and, where exposed, shall match adjoining surfaces in texture and color. White portland cement shall be used as needed to attain color match.
- B. Formed Surfaces: Fins and loose material shall be removed. Unsound concrete, voids over 1/2 inch in diameter, and tie-rod and bolt holes shall be cut back to solid concrete, reamed, brushed-coated with cement grout, and filled solid with a stiff portland-cement-sand mortar mix.
- C. Unformed Surfaces: Surfaces shall be finished to a true plane with no deviation exceeding 1/4 inch when tested with a 10-foot straightedge. Surfaces shall be pitched to drains. Surfaces shall be screeded and floated to the required level with no coarse aggregate visible before finishing as specified below.
 - 1. Monolithic Finish: Monolithic finish shall be given to slabs unless otherwise specified. After the surface moisture has disappeared, floated-surfaces shall be steel-troweled to a smooth, even, dense finish free from blemish including trowel marks.
 - 2. Nonslip Finish: Nonslip finish shall be given to stair treads, landings, exterior building entrances, vestibules, and other surfaces so indicated by brooming with a fiber-bristle brush in a direction transverse to that of main traffic.

3.07 CURING:

- A. General: Concrete shall be cured by protection against loss of moisture and rapid temperature changes for a period of not less than 7 days from the beginning of the curing operation. Unhardened concrete shall be protected from rain and flowing water. The Contractor shall have all equipment needed for adequate curing and protection of the concrete on hand and ready to install before actual

concrete placement begins. Failure to comply with curing requirements shall be cause for immediate suspension of concreting operations.

B. **Burlap Curing:** Immediately after the finishing operations have been completed and the concrete has set sufficiently to prevent marring the surface, the entire surface of the newly laid concrete shall be covered with approved wetted burlap that shall be kept wet for a period of not less than 24 hours. The surface of the newly laid concrete shall be kept moist until the burlap coverings are in place. Curing of the concrete shall be continued for the duration of the required curing period by this method or one of the methods specified below.

1. **Waterproof-Paper Blankets or Impermeable Sheets:** Immediately after removing the covering used for initial curing, the exposed concrete surfaces shall be moistened with a fine spray of water and then covered with waterproof-paper blankets, polyethylene-coated-burlap blankets, or impermeable sheets. Burlap of polyethylene-coated-burlap shall be saturated with water before placing. Sheets shall be placed with the light-colored side up. Sheets shall overlap not less than 12 inches with edges taped or secured to form a completely closed joint. Coverings shall be weighted down to prevent displacement or billowing from winds. Tears or holes appearing during the curing period shall be immediately repaired by patching.

2. **Membrane-forming curing compound** shall be applied immediately to exposed concrete surfaces after removing burlap coverings. The curing compound shall be applied with an overlapping coverage that will give a two-coat application at a coverage of not more than 200 square feet per gallon for both coats. When application is made by hand-operated sprayers, the second coat shall be applied in a direction approximately at right angles to the first coat. The compound shall form a uniform, continuous, cohesive film that will not check, crack, or peel, and that will be free from pinholes and other imperfections. Concrete surfaces that are subjected to heavy rainfall within 3 hours after the curing compound has been applied shall be resprayed at the coverage specified above and at no additional cost to the Government. Areas covered with curing compound that are damaged by subsequent construction operations within the specified curing period shall be resprayed at no additional cost to the Government.

3.08 **FINISH TOLERANCE:** THE FINISHED SURFACES OF PATCHED AREAS SHALL MEET THE FACE OF THE adjoining surfaces and shall not deviate more than 1/4 inch from a true plane surface within the patched area.

3.09 **SURFACE PROTECTION:** THE CONTRACTOR SHALL PROTECT THE PATCHED AREAS AGAINST damage prior to final acceptance of the work by the Government. Traffic shall be excluded from the patched areas by erecting and maintaining barricades and signs until the completion of the curing period of the concrete.

3.10 REINFORCING STEEL REPAIR AND REPLACEMENT

A. Steel shall be accurately set to match the original lines and spacing and shall be securely held in place with standard spacers, chairs or other approved supports. Reinforcing shall be installed according to ACI 318.

B. Remove corrosion from all reinforcing steel exposed after removal of concrete. Apply a protective coating to the steel and coat with epoxy prior to placement of new concrete.

C. Replace severely corroded reinforcing steel with new reinforcing steel welded to the existing non-deteriorated portions.

3.11 SEALANT REPLACEMENT

- A. Missing or deteriorated caulking and sealants in contact areas between concrete and other materials (i.e., window and door frames, expansion joints, etc.) shall be replaced.
1. If the sealant is missing, a full bead of elastic sealant compound shall be placed in the open joints.
 2. If a sealant material was installed, but has torn, deteriorated or lost elasticity, it shall be carefully cut out. The opening must be cleaned of all old sealant material. New sealant shall then be placed in the clean joint.
 3. All joints shall be properly primed before the new sealant material is applied.
 4. A backer rod material shall be placed in all joints deeper than 3/4" (19 mm) or wider than 3/8" (10 mm).

END OF SECTION

SECTION 04250

MASONRY REPAIR

PART 1 - GENERAL

1.01 WORK INCLUDED:

- A. Removal of masonry units where noted on drawings.
- B. New concrete unit masonry.
- C. Minor removal of deteriorated concrete and patching to restore sound structural surfaces.
- D. Removal and replacement of steel lintels.
- E. New masonry reinforcement and accessories.
- F. Temporary shoring and protection of existing materials and equipment.

1.02 RELATED WORK

- A. Section: none

1.03 PROJECT DELIVERY, STORAGE AND PROTECTION

- A. Deliver cement and lime materials in unopened containers.
- B. Store materials in a dry place with elevated floors and cover with canvas or polyethylene. No material shall be used where bag or container shows watermarks.

1.04 JOB CONDITIONS

- A. Do not put antifreeze or accelerating admixtures in any mortar used in masonry. Masonry work performed in, near or below freezing weather, shall be done in heated enclosures.
- B. Calcium chloride not permitted.

1.05 REFERENCE STANDARDS

- A. ASTM C129 Hollow Non-Load Bearing Concrete Masonry Units
- B. ASTM C90 Hollow Load Bearing Concrete Masonry Units
- C. ANSI A41.1 Building Code Requirements for Masonry
- D. ASTM C145 Solid Load Bearing Concrete Masonry Units
- E. ASTM C150 Portland cement
- F. ASTM C91 Masonry cement
- G. ASTM C207 Lime
- H. ASTM C144 Sand

PART 2 - PRODUCTS

2.01 MASONRY

- A. Concrete Blocks: ASTM C129 Hollow Core Non-Load Bearing Grade N, Type I, size as required, complete with corners, bases, bond beams, lintels and fillers to match and compliment block units.

2.02 MORTAR MATERIALS AND MIXES

- A. Portland Cement: ASTM C150 normal-type I; color to match existing.
- B. Lime: ASTM C207, Type S.
- C. Sand: ASTM C144.
- D. Water: Drinkable, from a public source.
- E. Waterproofing admixture: Euclid Chemical "Integral Waterpeller", Master Builders "Omicron" or Sonneborn-Contech "Hydrocide" (for exterior masonry work only).
- F. Type S mortar: ASTM C270 proportions by volume, 1 part portland cement, 1/2 part hydrated lime and not more than 4 1/2 parts sand, measured in a damp, loose condition with a minimum average compressive strength at 28 days of 1800 psi. Type S mortar may be 1/2 part portland cement, 1 part masonry cement and not more than 4 1/2 parts sand.

2.03 MASONRY REINFORCEMENT AND ACCESSORIES

- A. Wall Ties; Corrosion resistant material furnished and installed in accordance with Technical Note 44 B published by the Brick Institute of America, 1986 Edition.
- B. Fasteners; Corrosion resistant material furnished and installed in accordance with Technical Note 44 A, published by The Brick Institute of America, 1986 Edition.
- C. Anchor Bolts; Conventional or proprietary bolts furnished and installed in accordance with Technical Note 44 published by The Brick Institute of America, 1986 Edition.
- D. Lintel; ASTM A-36 structural steel with galvanized coating.

2.04 CONCRETE PATCHING MATERIAL

- A. Concrete Bonding Agent; Sonneborn "Sonobond"; two-component, 100% epoxy resin, adhesive system.
- B. Concrete Patching Material; Sonneborn "Epolith Patcher", two component, aggregate filled, epoxy resin patching compound.

2.05 MISCELLANEOUS MATERIAL

- A. Sealant; TREMCO Dymonic 1-component moisture curing polyurethane joint sealant, TT-S-00230C, Type II, Class A or TREMCO Dymeric 3 part epoxidized polyurethane terpolymer sealant TT-S-00227E, Type II, Class A.

PART 3 - EXECUTION

3.01 GENERAL REQUIREMENTS

- A. Temperature; Masonry work shall not take place when temperature falls below 30 degrees Fahrenheit unless adequate protective measures are taken. Masonry units that are coated with frost and ice shall not be incorporated into walls.
- B. Excessively wet concrete masonry units shall not be used.
- C. Cutting of all masonry units shall be done with power equipment; cut edges to be free of chipping damage.
- D. Each masonry unit shall be adjusted to its final position while mortar is still plastic. Remove and relay any unit with fresh mortar that is disturbed after mortar has hardened.
- E. Masonry units that are cracked shall not be laid. Those having small chips and spawls may be used in concealed locations.
- F. It is intended that lintels occur at a regular joint level, adjust as necessary to provide this wherever possible. Set lintels with equal bearing at each end, completely embed in masonry.
- G. Clean masonry walls and adjacent surfaces daily as work progresses, remove mortar droppings and smears before they harden. At completion of masonry work, clean concrete masonry with a 10% solution of muratic acid and a stiff brush; wash clean with clear water. Remove all excess mortar from face of masonry.

3.02 MIXING MORTAR

- A. Mortar mix may be varied with project inspector's permission depending on atmospheric and ambient conditions. Use only accurate measuring devices.
- B. Mix all cementitious materials and sand in a mechanical batch mixer for a minimum of 5 minutes. Adjust the consistence of the mortar to the satisfaction of mason but add only as much water as is compatible with convenience in using the mortar. If the mortar begins to stiffen from evaporation or from absorption of a part of the mixing water, retemper the mortar immediately by initial mixing. Do not use mortar after it has begun to set.
- C. Add admixtures to mortar in strict accordance with manufacturer's recommendations.
- D. Use Type S mortar (1800 psi) for all masonry work.

3.03 - MASONRY REPAIR

- A. Sealant Replacement
 - 1. Missing or deteriorated caulking and sealants in contact areas between masonry units and other materials, i.e., window and door frames, expansion joints, etc., shall be inspected. If the sealant is missing, a full bead of elastic sealant compound shall be placed in the open joints. If a sealant material was installed, but has torn, deteriorated or lost elasticity, it shall be carefully cut out. The opening must be cleaned of all old sealant material. New sealant shall then be placed in the clean joint. All joints shall be properly primed before the new sealant material is applied. A backer rod material shall be placed in all joints deeper than 3/4" or wider than 3/8".

END OF SECTION

SECTION 05055

WELDING, STRUCTURAL

PART 1 - GENERAL

1.01 SCOPE OF WORK

- A. Work includes, but is not limited to the following:
 - 1. For any repair or patchwork needed as a result of items being demolished.

1.02 APPLICABLE PUBLICATIONS

- A. The publications listed below form a part of this specification to the extent referenced. The publications are referred to in the text by basic designation only.

AMERICAN INSTITUTE OF STEEL CONSTRUCTION (AISC)

- AISC-04 Specification for Structural Steel Buildings - Allowable Stress Design, Plastic Design

AMERICAN SOCIETY FOR NONDESTRUCTIVE TESTING (ASNT)

- ASNT-01 Recommended Practice SNT-TC-1A

AMERICAN WELDING SOCIETY (AWS)

- AWS A2.4 Standard Symbols for Welding, Brazing and Nondestructive Examination
- AWS A3.0 Standard Welding Terms and Definitions
- AWS D1.1 Structural Welding Code - Steel
- AWS Z49.1 Safety in Welding and Cutting and Allied Processes

1.03 DEFINITIONS

- A. Definitions of welding terms shall be in accordance with AWS A3.0.

1.04 GENERAL REQUIREMENTS

- A. The design of welded connections shall conform to AISC-04 unless otherwise indicated or specified. Material with welds will not be accepted unless the welding is specified or indicated on the drawings or otherwise approved. Welding shall be as specified in this section, except where additional requirements are shown on the drawings or are specified in other sections. Welding shall not be started until welding procedures, welders, welding operators, and tackers have been qualified and the submittals approved by the Contracting Officer. Qualification testing shall be performed at or near the work site. Each Contractor performing welding shall maintain records of the test results obtained in welding procedure, welder, welding operator, and tacker performance qualifications.

1.05 SUBMITTALS

- A. Statements

1. Welding Procedure Qualifications
2. Welder, Welding Operator, and Tacker Qualification
3. Inspector Qualification
4. Copies of the welding procedure specifications; the procedure qualification test records; and the welder, welding operator, or tacker qualification test records.

B. Records

1. Quality Control: A quality assurance plan and records of tests and inspections.

1.06 WELDING PROCEDURE QUALIFICATIONS

A. Except for prequalified (per AWS D1.1) and previously qualified procedures, each Contractor performing welding shall record in detail and shall qualify the welding procedure specification for any welding procedure followed in the fabrication of weldments. Qualification of welding procedures shall conform to AWS D1.1 and to the specifications in this section. Copies of the welding procedure specification and the results of the procedure qualification test for each type of welding which requires procedure qualification shall be submitted for approval. Approval of any procedure, however, will not relieve the Contractor of the sole responsibility for producing a finished structure meeting all the requirements of these specifications. This information shall be submitted on the forms in Appendix E of AWS D1.1. Welding procedure specifications shall be individually identified and shall be referenced on the detail drawings and erection drawings, or shall be suitably keyed to the contract drawings. In case of conflict between this specification and AWS D1.1, this specification governs.

1. Previous Qualifications: Welding procedures previously qualified by test may be accepted for this contract without requalification if the following conditions are met:
 - a. Testing was performed by an approved testing laboratory, technical consultant, or the Contractor's approved quality control organization.
 - b. The qualified welding procedure conforms to the requirements of this specification and is applicable to welding conditions encountered under this contract.
 - c. The welder, welding operator, and tacker qualification tests conform to the requirements of this specification and are applicable to welding conditions encountered under this contract.
2. Prequalified Procedures: Welding procedures which are considered prequalified as specified in AWS D1.1 will be accepted without further qualification. The Contractor shall submit for approval a listing or an annotated drawing to indicate the joints not prequalified. Procedure qualification shall be required for these joints.
3. Retests: If welding procedure fails to meet the requirements of AWS D1.1, the procedure specification shall be revised and requalified, or at the Contractor's option, welding procedure may be retested in accordance with AWS D1.1. If the welding procedure is qualified through retesting, all test results, including those of test welds that failed to meet the requirements, shall be submitted with the welding procedure.

1.07 WELDER, WELDING OPERATOR, AND TACKER QUALIFICATION

- A. Each welder, welding operator, and tacker assigned to work on this contract shall be qualified in accordance with the applicable requirements of AWS D1.1 and as specified in this section. Welders, welding operators, and tackers who make acceptable procedure qualification test welds will be considered qualified for the welding procedure used.
1. Previous Qualifications: At the discretion of the Contracting Officer, welders, welding operators, and tackers qualified by test within the previous 6 months may be accepted for this contract without requalification if all the following conditions are met:
 - a. Copies of the welding procedure specifications, the procedure qualification test records, and the welder, welding operator, and tacker qualification test records are submitted and approved in accordance with the specified requirements for detail drawings.
 - b. Testing was performed by an approved testing laboratory, technical consultant, or the Contractor's approved quality control organization.
 - c. The previously qualified welding procedure conforms to the requirements of this specification and is applicable to welding conditions encountered under this contract.
 - d. The welder, welding operator, and tacker qualification tests conform to the requirements of this specification and are applicable to welding conditions encountered under this contract.
 2. Certificates: Before assigning any welder, welding operator, or tacker to work under this contract, the Contractor shall submit the names of the welders, welding operators, and tackers to be employed, and certification that each individual is qualified as specified. The certification shall state the type of welding and positions for which the welder, welding operator, or tacker is qualified, the code and procedure under which the individual is qualified, the date qualified, and the name of the firm and person certifying the qualification tests. The certification shall be kept on file, and 3 copies shall be furnished. The certification shall be kept current for the duration of the contract.
 3. Renewal of Qualification: Requalification of a welder or welding operator shall be required under any of the following conditions:
 - a. It has been more than 6 months since the welder or welding operator has used the specific welding process for which he is qualified.
 - b. There is specific reason to question the welder or welding operator's ability to make welds that meet the requirements of these specifications.
 - c. The welder or welding operator was qualified by an employer other than those firms performing work under this contract, and a qualification test has not been taken within the past 12 months. Records showing periods of employment, name of employer where welder, or welding operator, was last employed, and the process for which qualified shall be submitted as evidence of conformance.
 - d. A tacker who passes the qualification test shall be considered eligible to perform tack welding indefinitely in the positions and with the processes for which he is qualified, unless there is some specific reason to question the tacker's ability. In such a case, the tacker shall be required to pass the prescribed tack welding test.

1.08 INSPECTOR QUALIFICATION

- A. Inspection and nondestructive testing personnel shall be qualified in accordance with the requirements of ASNT-01 for Levels I or II in the applicable nondestructive testing method. The inspector may be supported by assistant welding inspectors who are not qualified to ASNT-01, and assistant inspectors may perform specific inspection functions under the supervision of the qualified inspector.

1.09 SYMBOLS

- A. Symbols shall be in accordance with AWS A2.4, unless otherwise indicated.

1.10 SAFETY

- A. Safety precautions during welding shall conform to AWS Z49.1.

PART 2 - PRODUCTS

2.01 WELDING EQUIPMENT AND MATERIALS

- A. All welding equipment, electrodes, welding wire, and fluxes shall be capable of producing satisfactory welds when used by a qualified welder or welding operator performing qualified welding procedures. All welding equipment and materials shall comply with the applicable requirements of AWS D1.1.

PART 3 - EXECUTION

3.01 WELDING OPERATIONS

- A. Requirements: Workmanship and techniques for welded construction shall conform to the requirements of AWS D1.1 and AISC-04. When AWS D1.1 and the AISC-04 specification conflict, the requirements of AWS D1.1 shall govern.
- B. Identification: Welds shall be identified in one of the following ways:
 - 1. Written records shall be submitted to indicate the location of welds made by each welder, welding operator, or tacker.
 - 2. Each welder, welding operator, or tacker shall be assigned a number, letter, or symbol to identify welds made by that individual. The Contracting Officer may require welders, welding operators, and tackers to apply their symbol next to the weld by means of rubber stamp, felt-tipped marker with waterproof ink, or other methods that do not cause an indentation in the metal. For seam welds, the identification mark shall be adjacent to the weld at 1 meter 3 foot intervals. Identification with die stamps or electric etchers shall not be allowed.

3.02 QUALITY CONTROL

- A. Testing shall be done by an approved inspection or testing laboratory or technical consultant, or if approved, the Contractor's inspection and testing personnel may be used instead of the commercial inspection or testing laboratory or technical consultant. The Contractor shall perform visual inspection to determine conformance with paragraph STANDARDS OF ACCEPTANCE. Procedures and techniques for inspection shall be in accordance with applicable requirements of AWS D1.1, except that in radiographic inspection only film types designated as "fine grain," or "extra fine," shall be employed.

3.03 STANDARDS OF ACCEPTANCE

- A. Dimensional tolerances for welded construction, details of welds, and quality of welds shall be in accordance with the applicable requirements of AWS D1.1 and the contract drawings. Nondestructive testing shall be by visual inspection method. The minimum extent of nondestructive testing shall be random 10 percent of welds or joints, as indicated on the drawings.
 - 1. Nondestructive Examination: The welding shall be subject to inspection and tests in the mill, shop, and field. Inspection and tests in the mill or shop will not relieve the Contractor of the responsibility to furnish weldments of satisfactory quality. When materials or workmanship do not conform to the specification requirements, the Government reserves the right to reject material or workmanship or both at any time before final acceptance of the structure containing the weldment.
 - 2. Destructive Tests: When metallographic specimens are removed from any part of a structure, the Contractor shall make repairs. The Contractor shall employ qualified welders or welding operators, and shall use the proper joints and welding procedures, including peening or heat treatment if required, to develop the full strength of the members and joints cut and to relieve residual stress.

3.04 GOVERNMENT INSPECTION AND TESTING

- A. In addition to the inspection and tests performed by the Contractor for quality control, the Government will perform inspection and testing for acceptance to the extent determined by the Contracting Officer. The costs of such inspection and testing will be borne by the Contractor if unsatisfactory welds are discovered, or by the Government if the welds are satisfactory. The work may be performed by the Government's own forces or under a separate contract for inspection and testing. The Government reserves the right to perform supplemental nondestructive and destructive tests to determine compliance with paragraph STANDARDS OF ACCEPTANCE.

3.05 CORRECTIONS AND REPAIRS

- A. When inspection or testing indicates defects in the weld joints, the welds shall be repaired using a qualified welder or welding operator as applicable. Corrections shall be in accordance with the requirements of AWS D1.1 and the specifications. Defects shall be repaired in accordance with the approved procedures. Defects discovered between passes shall be repaired before additional weld material is deposited. Wherever a defect is removed and repair by welding is not required, the affected area shall be blended into the surrounding surface to eliminate sharp notches, crevices, or corners. After a defect is thought to have been removed, and before rewelding, the area shall be examined by suitable methods to insure that the defect has been eliminated. Repair welds shall meet the inspection requirements for the original welds. Any indication of a defect shall be regarded as a defect, unless reevaluation by nondestructive methods or by surface conditioning shows that no unacceptable defect is present.

END OF SECTION

SECTION 07213

FIBROUS BATT INSULATION

PART 1 - GENERAL

1.01 WORK INCLUDED

- A. Batt insulation for sound barrier walls (if required).
- B. Wire mesh for holding insulation in place.

1.02 REFERENCE STANDARDS

- A. ASTM C 665 - Insulation Blankets, Thermal Fiber, for Ambient Temperatures.

PART 2 - PRODUCTS

2.01 MATERIALS

- A. Noise Barrier Insulation: Preformed mineral wool conforming to ASTM C 665; Unfaced; 3" or more thick; R-11.
- B. Nails or staples: Of galvanized steel wire, type and size as recommended for application.
- C. Wire Mesh: 20 gage wire with 1-inch mesh openings.

PART 3 - EXECUTION

3.01 WORKMANSHIP

- A. Install batt insulation in accordance with manufacturer's recommendations. Install after mechanical and electrical services within walls have been installed.
- B. Fit insulation tight within spaces and tight to and behind mechanical and electrical services within the plane of insulation. Leave no gaps or voids.

3.02 INSTALLATION

- A. Install insulation above suspended ceilings in sizes to match ceiling pad dimensions, with factory applied membrane facing warm side of building.

END OF SECTION

SECTION 08700

HARDWARE

PART 1 - GENERAL

1.01 WORK INCLUDED

- A. Hardware for doors and acoustic seals.

1.02 REFERENCE STANDARDS

- A. FS: FF-H-106 Locks and door trim
- B. FS: FF-H-111 Shelf and miscellaneous
- C. FS: FF-H-116 Hinges
- D. FS: FF-H-121 Door closing devices

1.03 SUBMITTALS

- A. Hardware - Catalog cuts and schedule.

1.04 KEYING

- A. Rim cylinders shall be interchangeable core, 7 pin tumbler, Federal Stock Series 5340, locking mechanism type P11C7R1 as manufactured by Best Lock Company. Cylinder mortise for interior doors shall be 1E74, 7 pin tumbler. Furnish 2 blank keys for each core. Cores and blank keys shall be turned into the base lock shop: Bldg 22, Area C 257-4893 or 257-4876. The Government shall install the permanent cores. Provide temporary cores as required for the protection of materials, equipment and work area.

PART 2 - PRODUCTS

2.01 HARDWARE

- A. Provide items as listed in the hardware sets and additional items not specifically called out to complete each door's hardware set to function as intended.

2.02 LOCKSET, LOCK TRIM AND DOOR TRIM

- A. Locks and latch sets: Series 1000
- B. Panic exits devices: Type 3

2.03 HINGES

- A. Hinges: Type T2107, size 4 1/2" x 4 1/2".
 - 1. All doors shall have non-removable pins.

2.04 MISCELLANEOUS

- A. Floor stop: Type 1311

2.05 DOOR CLOSING DEVICE

- A. Closers: Type 3012, size IV

2.06 THRESHOLD AND WEATHER STRIPPING

2.07 HARDWARE FINISHES

- A. Finish shall be US10 bronze or match existing.

PART 3 - EXECUTION

3.01 INSTALLATION

- A. Install hardware in accordance with manufacturer's recommendations, using proper templates unless detailed otherwise.
- B. Mounting heights shall be per industry standards unless otherwise noted.

3.02 HARDWARE SETS

- A. Hardware sets shall be as follows:

Hardware Group #1

- 1 Mortise/Electric Exit
Device Type 3-12 (Entrance by control lever only when released by turning key or activating electric access system; key removable only when locked; fail secure.)
(Keyed so lever cannot be left unlocked; fail secure.)
Power Transfer
- 2 Pair Butt (NRP) Hinges
- 1 Mortise OH Stop
- 1 Card Reader Door Controller (See SECTION: Card Access System)
- 1 Closer
- 1 Balanced Magnetic Switch
- 1 Set Acoustic Seals
- 1 Auto Door Bottom
- 1 Threshold-1/4" Aluminum, Smooth Surface
- 1 X0-8 Electromechanical Lock (high security pedestrian exit device)

NOTES:

Hardware, doors, detection switches, wiring and conduit shall meet the security requirements for a Sound Group 4 as outlined in paragraph 4 of Section 01020. Hardware and door assembly shall be provided as a package meeting FSTC specified in SECTION: Steel Doors and Frames

Hardware Group #2

See SECTION: Steel Doors
and Frames; Additional Hardware as Listed Below:

- 1 Mortise/Electric Exit
Device Type 3-12 (Entrance by control lever only when released by turning key or activating electric access system; key removable only when locked; fail secure.)
(Keyed so lever cannot be left unlocked; fail secure.)
Power Transfer
- 1 1/2 Pair Butt (NRP) Hinges
- 1 Wall Stop
- 1 Closer
- 1 Card Reader Door Controller (See SECTION: Card Access System)
- 1 Set Acoustic Seals
- 1 Auto Door Bottom
- 1 Threshold-1/4" Aluminum, Smooth Surface

NOTES:

Hardware, doors, detection switches, wiring and conduit shall meet the security requirements for a Sound Group 4 as outlined in DCID 1/21. Hardware and door assembly shall be provided as a package meeting FSTC specified in SECTION: Steel Doors and Frames

Hardware Group #3

- 1 F07 Storeroom Latchset
- 1 1/2 Pair Butt (NRP) Hinges
- 1 Wall Stop

Hardware Group #4

See SECTION: Steel Doors
and Frames; Additional Hardware as Listed Below:

- 1 Panic Device (Type 3, Function 01)
- 1 1/2 Pair Butt (NRP) Hinges
- 1 Closer with stop
- 1 Balanced Magnetic Switch
- 1 Set Acoustic Seals
- 1 Auto Door Bottom
- 1 Threshold-1/4" Aluminum, Smooth Surface

NOTES:

Hardware, doors, detection switches, wiring and conduit shall meet the security requirements for a Sound Group 4 as outlined in DCID 1/21 and door assembly shall be provided as a package meeting FSTC specified in SECTION: Steel Doors and Frames

Hardware Group #5

See SECTION: Steel Doors
and Frames; Additional Hardware as Listed Below:

- 1 Mortise/Electric Exit
Device Type 3-12 (Entrance by control lever only when released by turning key or activating electric access system; key removable only when locked; fail secure.)
(Keyed so lever cannot be left unlocked; fail secure.)
Power Transfer
- 2 Pair Butt (NRP) Hinges
- 1 Wall Stop
- 1 Closer
- 1 Card Reader Door Controller (See SECTION: Card Access System)
- 1 Set Acoustic Seals
- 1 Auto Door Bottom
- 1 Threshold-1/4" Aluminum, Smooth Surface

NOTES:

Hardware, doors, detection switches, wiring and conduit shall meet the security requirements for a Sound Group 4 as outlined in DCID 1/21. Hardware and door assembly shall be provided as a package meeting FSTC specified in SECTION: Steel Doors and Frames

END OF SECTION

SECTION 11132

PROJECTION SCREENS

PART 1 - GENERAL

1.01 SUMMARY

- A. Section Includes
 - 1. Front-projection screens
- B. Related Sections
 - 1. 06100 - Rough Carpentry
 - 2. 09250 - Gypsum Board
 - 3. 09510 – Acoustic Ceilings
 - 4. Division 16 - Electrical connections

1.02 SUBMITTALS

- A. Product Data: For each type of screen indicated. Include manufacturer's specifications and installation instructions.
- B. Shop Drawings: Show layouts and types of projection screens. Include the following:
 - 1. Location of screen centerline relative to ends of screen case.
 - 2. Connections to supporting structure for pendant- and recess-mounted screens.
 - 3. Anchorage details.

1.03 QUALITY ASSURANCE

- A. Source Limitations: Obtain projection screens through one source from a single manufacturer. Obtain each screen as a complete unit, including necessary mounting hardware and accessories.
- B. Electrical Components, Devices, and Accessories: Listed and labeled as defined in NFPA 70, Article 100, by a testing agency acceptable to authorities having jurisdiction, and marked for intended use.

1.04 DELIVERY, STORAGE AND HANDLING

- A. Do not deliver projection screens until construction within spaces where screens will be installed is substantially complete and ready for screen installation.

PART 2 - PRODUCTS

2.01 FRONT PROJECTION SCREENS

- A. Manually Operated Screens, General: Manufacturer's standard spring-roller-operated units, consisting of case, screen, mounting accessories, and other components necessary for a complete installation.
 - 1. Screen Mounting: Top edge securely anchored to a 3-inch- (75-mm-) diameter, rigid steel roller; bottom edge formed into a pocket holding a tubular metal slat, with ends of slat protected by plastic caps, and with a saddle and pull attached to slat by screws.

PROJECTION SCREENS

2. Tab Tensioning: Units have stainless-steel tensioning cables on both sides of screen connected to edges of screen by tabs to pull screen flat horizontally.
- B. Electrically Operated Screens, General: Manufacturer's standard units consisting of case, screen, motor, controls, mounting accessories, and other components necessary for a complete installation. Provide units that are listed and labeled as an assembly by UL or another testing and inspecting agency acceptable to authorities having jurisdiction.
1. Low-Voltage Control: System consisting of a control unit with 24-V power supply, remote 3-button or 3-position switches, and interconnecting wiring. Provide infrared remote control consisting of battery-powered transmitter and receiver for use with low-voltage control system.
 2. Motor in Roller: Instant-reversing motor of size and capacity recommended by screen manufacturer; with permanently lubricated ball bearings, automatic thermal-overload protection, preset limit switches to automatically stop screen in up and down positions, and positive-stop action to prevent coasting. Mount motor inside roller with vibration isolators to reduce noise transmission.
 3. End-Mounted Motor: Instant-reversing, gear-drive motor of size and capacity recommended by screen manufacturer; with permanently lubricated ball bearings, automatic thermal-overload protection, preset limit switches to automatically stop screen in up and down positions, and positive-stop action to prevent coasting.
 5. Screen Mounting: Top edge securely anchored to rigid metal roller and bottom edge formed into a pocket holding a 3/8-inch diameter metal rod with ends of rod protected by plastic caps.
 - a. Roller for end-mounted motor supported by self-aligning bearings in brackets.
 - b. Roller for motor in roller supported by vibration- and noise-absorbing supports.
 6. Tab Tensioning: Units have stainless-steel tensioning cables on both sides of screen connected to edges of screen by tabs to pull screen flat horizontally.
- C. Surface-Mounted, Metal Encased, Manually Operated Screens: Units designed and fabricated for surface mounting on wall or ceiling, fabricated from formed steel sheet not less than 0.027 inch thick or aluminum extrusions; with flat back design and vinyl covering or baked-enamel finish. Provide end caps and universal mounting brackets, finished to match end caps.
- D. Recessed, Electrically Operated Screens with Automatic Ceiling Closure: Motor in roller or end-mounted motor units designed and fabricated for recessed installation in ceiling; with bottom of case composed of two panels fully enclosing screen, motor, and wiring, one panel hinged and designed to open and close automatically when screen is lowered and fully raised, the other removable or openable for access to interior of case.
1. Provide metal or metal-lined motor enclosure on units with end-mounted motor.
 2. Provide metal or metal-lined wiring compartment on units with motor in roller.
 3. Screen Case: Made from metal and fire-retardant materials.
 4. Provide screen case with trim flange to receive ceiling finish.
 5. Prime paint surfaces of screen case that will be exposed to view in the finished work.
- E. Screen Material and Viewing Surface:
1. Glass-Beaded Viewing Surface: Peak gain of 2.0 to 2.8, and half-gain angle of at least 15 degrees.
 2. Mildew Resistance: Rating of 0 or 1 when tested according to ASTM G 21.
 3. Flame Resistance: Passes NFPA 701.
 4. Flame-Spread Index: Not greater than 75 when tested according to ASTM E 84.
 5. Seamless Construction: Provide screens, in sizes indicated, without seams.
 6. Edge Treatment: Black masking borders.
 7. Size of Viewing Surface: 72 by 96 inches.

PROJECTION SCREENS

PART 3 - EXECUTION

3.01 EXAMINATION

- A. Examine areas and conditions to which projection screens installed. Do not proceed with work until unsatisfactory conditions are corrected.

3.02 INSTALLATION

- A. General: Install projection screens at locations indicated to comply with screen manufacturer's written instructions.
- B. Install front-projection screens with screen cases in position and in relation to adjoining construction indicated. Securely anchor to supporting substrate in a manner that produces a smoothly operating screen with vertical edges plumb and viewing surface flat when screen is lowered.
 - 1. Install low-voltage controls according to NFPA 70 and manufacturer's written instructions.
 - a. Wiring Method: Install wiring in raceway except in accessible ceiling spaces and in gypsum board partitions where unenclosed wiring method may be used. Use UL-listed plenum cable in environmental air spaces, including plenum ceilings. Conceal raceway and cables except in unfinished spaces.
 - 2. Test electrically operated units to verify that screen controls, limit switches, closure, and other operating components are in optimum functioning condition.
 - 3. Test manually operated units to verify that screen operating components are in optimum functioning condition.

3.03 ADJUSTING

- A. After installation, protect projection screens from damage during construction. If damage occurs despite such protection, remove and replace damaged components or entire unit as required to provide units in their original, undamaged condition.

END OF SECTION

SECTION S15951A

ADDITIONS TO THE DIRECT DIGITAL CONTROL FOR HVAC FOR SCIF

PART 2 PRODUCT

2.1 Air Quality Sensor (Room)

Wall mounted sensor, aesthetically designed and suitable for installation in an office. Air quality sensor shall be non-dispersive infrared sensing type. Unit shall be microprocessor based with a 4 to 20 milliamp linear output. Range of operation shall be 0 to 2000 ppm CO2 with a setpoint of 1000 ppm CO2. Sensor/transducer accuracy shall be +/- 5% of reading or +/- 75 ppm CO2; maximum annual drift +/- 75 ppm CO2. Unit shall be field calibratable with span gas.

Provide a (LED) readout on the sensor/transducer to display the CO2 concentration being sensed. The readout shall continuously display the present value of Carbon Dioxide sensed.

Provide a field adjustable relay output on the Carbon Dioxide sensor/transducer. The actuation point of the relay shall be field adjustable from 700 to 130 ppm of CO2. The relay contacts shall have a minimum rating of 2 amps at VAC, non inductive.

PART 3 EXECUTION

3.1 CONTROL SEQUENCES OF OPERATION

3.1.1 General Requirements - HVAC Systems

These requirements shall apply to all primary HVAC systems unless modified herein. The sequences describe the actions of the control system for one direction of change in the HVAC process analog variable, such as temperature, humidity or pressure. The reverse sequence shall occur when the direction of change is reversed.

3.1.2 Strategy

Sequences described are pertinent to a specific control strategy. These strategies are keyed to control drawings to establish which strategies apply to various control systems.

3.1.3 Sequence of Operation

3.1.3.1 Start/Stop, AHU and RF

a. With the H-O-A switch on the starter panel in the "H" position, the unit will start when the appropriate safeties are satisfied.

b. With the H-O-A switch in the "A" position, the unit will operate in response to DDC control and system safety circuits.

3.1.3.2 Optimum Start (OST), AHU, RF and Terminal Units

- a. Scheduled start time, controlled by the DDC controller, can be altered by controllers optimum start program calculation.
- b. The result of the calculation is to compute the equipment start time so that the space temperature can be moved from its unoccupied mode setting, to the occupied mode setting for the space controlled, early enough to meet the scheduled start time for the space.

3.1.3.3 Optimum Stop (OSP), AHU, RF and Terminal Units

- a. Scheduled stop time, controlled by the DDC controller, can be altered by controllers optimum start/stop program.
- b. The result of the calculation is to compute the equipment stop time, so that the space temperature is allowed to drift from its occupied mode setting for the space controlled, to the upper or lower temperature limit by the scheduled stop time.

3.1.3.4 Unoccupied Mode (UM), AHU, RF and Terminal Units

- a. DDC controller will cause the AHU's, RF's and terminal units to go to unoccupied mode settings when called for by the schedule Start/Stop program.
- b. Space temperature settings to be reset to 55 deg F minimum and 90 deg F maximum.
- c. Outside air dampers shall close and the return air damper shall open.
- d. During heating season, the DDC shall cycle the AHU's and RF's to prevent the space temperature from falling below the minimum setpoint. The outside air damper shall remain closed and the return air damper shall remain open.

3.1.3.5 Occupied Mode (OM), AHU, RF and Terminal Units

- a. DDC controller will cause the AHU and RF to start and run continuously and controls to be energized.
- b. Space temperature setpoints to be reset to comfort levels (70 deg F minimum and 75 deg F maximum).
- c. Outside air and return air dampers to maintain minimum set air flow or position.
- d. Supply and exhaust fans listed on the control drawings as fans associated with air handling unit, shall be on.

3.1.3.6 Temperature Economizer Control (TEC), AHU and RF

- a. DDC controller to modulate outside air damper and the return air damper to achieve mixed air temperature setpoint.

b. When the outside air temperature is greater than the return air temperature, the economizer outside air damper shall close.

c. When the mixed air temperature (MAT) falls below setpoint, the economizer outside air damper shall close.

d. If the return air temperature is below an operator definable limit, then a warm-up cycle shall be initiated forcing the outside air dampers to their closed position and the return air damper in its open position. (See WARM-UP CYCLE) When return air temperature increases above the limit, plus a definable differential, then the warm-up cycle shall be terminated.

3.1.3.7 Warm-Up Cycle Control (WCC)

a. If the return air temperature is below setpoint 66 deg F, a "Warm-up" cycle shall initiate.

b. Outside air dampers will close and the return air damper shall open.

c. Heating control valve will open.

d. Terminal box reheat and reheat coils shall control to room temperature.

e. VAV BOX dampers shall control to room temperature.

f. When return air temperature increases above the limit, plus a definable differential, the warm-up cycle shall terminate.

3.1.3.8 Air Smoke Detection

a. Supply and return air duct smoke detector, upon sensing smoke, shall stop the AHU and RF through the electrical/fire alarm system and associated motor controller..

b. A set of NO contacts shall close and signal the Central Operating Terminal.

3.1.3.9 Filter Maintenance (FM)

a. Differential pressure switch with sensors on upstream and downstream side of filter will signal DDC controller when the differential pressure is equal to or greater than the setpoint.

b. DDC controller will initiate an alarm signal indicating a clogged filter and requirement for maintenance.

3.1.3.10 Supply Air Temperature (SAT) Control for Variable Volume AHU's

a. Supply air temperature (SAT) is reset down, when the setpoint deviates to the high side until all zone temperatures are satisfied. Conversely SAT is reset up as zone setpoints all deviate to the low side.

b. DDC controller shall reset the mixed air temp (MAT) control loop setpoint (Economizer control), to correlate to supply air temp (SAT) setpoint.

c. SAT shall modulate the cooling coil control loop to maintain SAT setpoint. The cooling coil face and bypass will be closed to the bypass under normal conditions.

d. MAT control loop shall modulate the economizer outdoor air damper to maintain MAT setpoint.

e. DDC controller shall modulate face and bypass air dampers and hot water coil valve in concert, at outdoor temperatures above 40 deg F to achieve SAT setpoint; and modulate the bypass damper only (coil valve at 100% open) when outdoor air temperatures are less than 40 deg F.

f. During summer the central heating system is off. If return air humidity rises above 65% the cooling coil valve will go full open to the cooling coil and the face and bypass dampers will modulate to maintain SAT.

3.1.3.11 Variable Speed Control (VSD), AHU SF

a. DDC controller will modulate fan speed with a 4-20 MA signal to variable frequency drive based on a differential pressure sensor, measuring pressure difference between supply duct pressure and space pressure.

b. As duct pressure decreases, fan speed will increase. As duct pressure increases, fan speed will decrease. On system failure VFD shall ramp down.

c. Air handling unit and associated fans and controls shall stop when fan differential pressure exceeds setpoint.

3.1.3.12 Variable Speed Control (VSD), AHU RF

a. DDC controller will modulate fan speed with a 4-20 MA signal to variable frequency drive based on a differential pressure sensor, measuring pressure difference between space pressure and outdoor pressure.

b. As space pressure increases, fan speed will increase. As space pressure decreases, fan speed will decrease. On system failure VFD shall ramp down.

c. The RF's shall run when their associated AHU runs except for as follows.

d. Return fan, AHU's and controls shall stop when fan differential pressure exceeds setpoint.

3.1.3.13 Minimum Outdoor Air (OA) Control for VAV AHU's

a. Occupied Mode: The minimum outdoor air and return air dampers will modulate in response to an OA flow measuring station to maintain a constant amount of OA. Upon a signal from the OA flow measuring station to increase flow the minimum outdoor air damper will open, when the minimum outdoor air damper is fully open and flow is not achieved then the return air damper will begin to close until minimum outdoor airflow is achieved. Minimum air flow quantity will be adjusted between the ranges listed based on the space air quality (AQ) sensors in the space. When any AQ sensor (Associated with VAV boxes served by any AHU) is not satisfied, the VAV boxes will first

modulate open. After it reaches its full open position the air handling units minimum outdoor airflow will be reset upward until it reaches the upper range listed. The return air damper will go to full open when the system is in Warm-Up Cycle Control or Unoccupied mode.

b. Unoccupied Mode: The minimum outdoor air damper will be closed; the return air damper will be open.

3.1.3.14 Freeze Stat Control

a. Air handling unit and associated fans and controls shall stop when freeze stat is tripped. Manual resetting or freeze stat is required to restart the System.

3.1.3.15 Terminal VAV BOX, Hydronic Reheat Coil, Control

a. DDC shall modulate variable volume damper and reheat coil valve in sequence to achieve space temperature setpoint.

b. When space temperature exceeds the cooling setpoint, the variable air volume (VAV) damper will modulate open. As the temperature falls VAV damper modulates to minimum position.

c. After damper reaches minimum position, the space temperature shall drift in a dead-band until reaching the heating control setpoint. As temperature continues to fall below setpoint, reheat coil valve shall modulate open.

d. A "high/low" position limit shall limit minimum and maximum air flow.

e. There are two temperature modes of operation for setpoints: one for "occupied" mode (73 +/- 3 degrees F adjustable) and one for "unoccupied" mode (heating = 55 degrees F, cooling = 90 degrees F, adjustable).

f. Where air quality sensor is shown next to a temperature sensor, the air quality sensor shall increase the airflow to the room when CO2 level exceeds 1000 ppm.

3.1.3.16 Status Indication

The DDC system shall monitor status points, listed in the I/O points list scheduled on the drawings and give indication of conditions (ie. On/Off, Start/Stop, Filter Clogged, etc.)

-- End of Section --

SECTION 16198B

DIRECTORIES FOR EXISTING PANELBOARDS

PART 1 - GENERAL

1.01 SECTION INCLUDES

- A. Provide typed directories in existing panelboards whose circuits are altered to indicate loads served by each circuit.

PART 2 - PRODUCTS

2.01 IDENTIFICATION

- A. Directories shall indicate load type and location for each circuit altered by this project.
- B. Information shall be copied from existing directories for all circuits not altered by this project.
- C. Use dash to indicate space or spare. Do not use words space or spare.
- D. At top of directory, indicate the following:
 - 1. Date directory was typed.
 - 2. Project number.
 - 3. Power source.
 - 4. Number and size of feeder conductors.

2.02 EXAMPLE

- A. An example follows:

Jan 87
Project WP 398-6
Fed by PDP-A
Feeder is (3) #2 AWG
1 Lights Rm 102
2 Receptacles Rm 109
etc

PART 3 - EXECUTION

3.01 HOLDERS

- A. Install each directory in holder behind transparent protective cover.

END OF SECTION

SECTION 16730A

INTRUSION DETECTION SYSTEM

PART 1 - GENERAL

1.01 SECTION INCLUDES

- A. Provide empty conduit and outlet boxes for intrusion detection systems for each protected area which include the following but are not limited to:
 - 1. Premises Control Unit
 - 2. Secondary Power Supply (Standby-Battery)
 - 3. Detectors
 - a. Balanced Magnetic Switches
 - b. Passive Infrared Motion Detector

1.02 DEFINITIONS

- A. Zone is defined as group of detectors which cover one protected volume.
- B. Intrusion Detection System is defined as system designed to detect unauthorized entry into protected , to detect removal of secured items, to alert police of intrusion, and to alert police of threat against personnel.

1.03 REFERENCES

- A. Underwriter's Laboratories, Incorporated (UL)
 - 1. 603 Power Supplies for use with Burglar Alarm Systems
 - 2. 634 Connectors and Switches for use with Burglar Alarm Systems
 - 3. 639 Intrusion Detection Units

END OF SECTION

UNCLASSIFIED

DIRECTOR
OF
CENTRAL
INTELLIGENCE
DIRECTIVE
1/21

PHYSICAL SECURITY
STANDARDS FOR
SENSITIVE
COMPARTMENTED
INFORMATION
FACILITIES (SCIF)

EFFECTIVE 29 JULY 1994

UNCLASSIFIED

UNCLASSIFIED

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

(Effective 29 July 1994)

PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES

Pursuant to the provisions of Section 102 of the National Security Act of 1947 and Executive Order 12333, physical security standards for sensitive compartmented information facilities (SCIFs) are hereby established.

1. PURPOSE

The purpose of this directive is to establish construction and security protection standards required for all US Government facilities or US Government-sponsored contractor facilities where sensitive compartmented information (SCI) may be stored, used, discussed, and/or processed.

2. GENERAL

All SCI must be stored within accredited SCIFs. Accreditation is the formal affirmation that the proposed facility meets physical security standards imposed by the DCI in the physical security standards manual that supplements this directive. The DCI is the accrediting authority for all SCIFs except where that authority has been delegated or otherwise provided for (see DCID 1/19).

3. APPLICABILITY

This directive is applicable to all SCIFs. Senior Officials of the Intelligence Community (SOICs) are charged with implementation and enforcement of the provisions of this directive. SCIFs established in all organizations outside the cognizance of Intelligence Community agencies/ departments as defined in Executive Order 12333 are directly under the authority and oversight of the DCI. SCIFs are established primarily for SCI and are intended to provide the highest level of physical security protection. It is sometimes necessary for non-SCI programs to be afforded an equal level of protection by introduction of such material into SCIFs. Should this occur, the express approval of the accrediting authority is required, and appropriate documentation shall be included in the accreditation records.

4. POLICY

SOICs shall establish and maintain within their agencies formal physical security programs to ensure that SCI is properly protected. The physical security requirements for such protection are contained in the Manual for Physical Security Standards for Sensitive Compartmented Information Facilities, the supplement to this directive. Annexes to this manual addressing specific technical and tactical applications of standards shall be published separately and periodically updated as required.

5. INTERPRETATION

Questions concerning the interpretation and implementation of SCIF physical security standards shall be referred to the Community Counterintelligence and Security Countermeasures Office/Intelligence Community Staff (CCISCMO/ICS) or successor organization.

UNCLASSIFIED

UNCLASSIFIED

DIRECTOR
OF
CENTRAL
INTELLIGENCE
DIRECTIVE
1/21

Manual for
PHYSICAL SECURITY
STANDARDS FOR
SENSITIVE
COMPARTMENTED
INFORMATION
FACILITIES (SCIF)

EFFECTIVE 30 JANUARY 1994

I
UNCLASSIFIED

UNCLASSIFIED

PREFACE:

DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities (SCIFs) was approved by the Director of Central Intelligence (DCI) on 30 January 1994.

A complete copy of DCID 1/21 consists of the basic DCID and annexes A through G. The annexes are as follows:

- Annex A - SCIF Checklist (approved 27 May 1994)
- Annex B - Alarms (approved 27 May 1994)
- Annex C - Tactical Operations/Field Training
(approved 27 May 1994)
 - Part I - Ground Operation
 - Part II - Aircraft/Airborne Operation
 - Part III - Shipborne Operation
- Annex D - Prohibited Items (approved 30 January 1994)
 - Part I - Electronic Equipment in SCIFs
 - Part II - Disposal of Laser Toner Cartridges
- Annex E - Acoustical control and Sound Masking Techniques
(approved 30 January 1994)
- Annex F - Personnel Access Controls (approved 30 January 1994)
- Annex G - Telephone Security (approved 29 July 1994)

UNCLASSIFIED

DCID 1/21

Table of Contents

PREFACE	
1. POLICY AND CONCEPT	1
1.1 Policy Statement	1
1.2 Concept	1
1.3 American Disabilities Act (ADA) Review	2
2. GENERAL/ADMINISTRATIVE	2
2.1 SCI Facilities (SCIFs)	2
2.2 Physical Security Preconstruction Review and Approval	2
2.3 Accreditation	3
2.4 Co-Utilization	4
2.5 Personnel Controls	4
2.6 Control of Combinations	5
2.7 Entry/Exit Inspections	5
2.8 Control of Electronic Devices and Other Items	5
3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SCIFs	6
3.1 Construction Policy for SCI Facilities	6
3.2 Temporary Secure Working Area (TSWA)	9
3.3 Requirements Common To All SCIFs	10
4. CONSTRUCTION SPECIFICATIONS	12
4.1 Vault Construction Criteria	12
4.2 SCIF Criteria For Permanent Dry Wall Construction	13
4.3 SCIF Construction Criteria For Steel Plate	13
4.4 SCIF Construction Criteria For Expanded Metal	13
4.5 General	13
GLOSSARY	14

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

(Effective 30 January 1994)

I. POLICY AND CONCEPT

1.1 Policy Statement

- 1.1.1 Physical security standards are hereby established governing the construction and protection of facilities for storing, processing, and discussing Sensitive Compartmented Information (SCI) which requires extraordinary security safeguards. Compliance with this DCID 1/21 Implementing Manual (hereafter referred to as the "Manual") is mandatory for all Sensitive Compartmented Information Facilities (SCIFs) established after the effective date of this manual, including those that make substantial renovations to existing SCIFs. Those SCIFs approved prior to the effective date of this Manual will not require modification to meet these standards.
- 1.1.2 The physical security safeguards set forth in this Manual are the standards for the protection of SCI. Senior Officials of the Intelligence Community (SOICs), with DCI concurrence, may impose more stringent standards if they believe extraordinary conditions and circumstances warrant. SOICs may not delegate this authority. Additional cost resulting from more stringent standards should be borne by the requiring Agency, Department, or relevant contract.
- 1.1.3 In situations where conditions or unforeseen factors render full compliance to these standards unreasonable, the SOIC or designee may waive specific requirements in accordance with this Manual. However, this waiver must be in writing and specifically state what has been waived. The Cognizant Security Authority (CSA) must notify all co-utilizing agencies of any waivers it grants.
- 1.1.4 All SCIFs must be accredited by the SOIC or designee prior to conducting any SCI activities.
- 1.1.5 One person is now authorized to staff a SCIF, which eliminates the two-person rule (the staffing of a SCIF with two or more persons in such proximity to each other to deter unauthorized copying or removal of SCI).

1.2 Concept

- 1.2.1 SCIF design must balance threats and vulnerabilities against appropriate security measures in order to reach an acceptable level of risk. Each security concept or plan must be submitted to the CSA for approval. Protection against surreptitious entry, regardless of SCIF location, is always required. Security measures must be taken to deter technical surveillance of activities taking place within the SCIF. TEMPEST security measures must be considered if electronic processing of SCI is involved.

- 1.2.2 On military and civilian compounds, there may exist security controls such as identification checks, perimeter fences, police patrols, and other security measures. When considered together with the SCIF location and internal security systems, those controls may be sufficient to be used in lieu of certain physical security or construction requirements contained in this Manual.
- 1.2.3 Proper security planning for a SCIF is intended to deny foreign intelligence services and other unauthorized personnel the opportunity for undetected entry into those facilities and exploitation of sensitive activities. Faulty security planning and equipment installation not only jeopardizes security but wastes money. Adding redundant security features causes extra expense which could be used on other needed features. When security features are neglected during initial construction, retrofitting of existing facilities to comply with security requirements is necessary.

1.3 American Disabilities Act (ADA) Review

- 1.3.1. Nothing in this manual shall be construed to contradict or inhibit compliance with the law or building codes. CSAs shall work to meet appropriate security needs according to the intent of this Manual at acceptable cost.

2. GENERAL/ADMINISTRATIVE

2.1 SCI Facilities (SCIFs)

A SCIF is an accredited area, room, group of rooms, buildings, or installation where SCI may be stored, used, discussed, and/or electronically processed. SCIFs will be afforded personnel access control to preclude entry by unauthorized personnel. Non-SCI indoctrinated personnel entering a SCIF must be continuously escorted by an indoctrinated employee who is familiar with the security procedures of that SCIF. The physical security protection for a SCIF is intended to prevent as well as detect visual, acoustical, technical, and physical access by unauthorized persons. Physical security criteria are governed by whether the SCIF is in the United States or not, according to the following conditions: closed storage, open storage, continuous operations, secure working area.

2.2 Physical Security Preconstruction Review and Approval

CSAs shall review physical security preconstruction plans for SCIF construction, expansion or modification. All documentation pertaining to SCIF construction will be appropriately controlled and restricted on a need-to-know basis. The approval or disapproval of a physical security preconstruction plan shall be made a matter of record.

- 2.2.1 The requester shall submit a Fixed Facility Checklist (FFC, Annex A) to the respective CSA for review and approval.
- 2.2.2 The Checklist submission shall include floor plans, diagrams of electrical, communications, heating, ventilation, air conditioning (HVAC) connections, security equipment layout (to include the location of intrusion detection equipment), etc. All diagrams or drawings must be submitted on legible and reproducible media.

UNCLASSIFIED

2.2.3 The CSA shall be responsible for providing construction advice and assistance and pre-approving SCIF construction or modification.

2.3 Accreditation

The CSA will ensure SCIFs comply with DCID 1/21. The CSA is authorized to inspect any SCIF, direct action to correct any deficient situation, and withdraw SCIF accreditation. The procedures for establishment and accreditation of SCIFs are prescribed below:

2.3.1 The procedures for establishment and accreditation of SCIFs from conception through construction must be coordinated and approved by the SOIC or CSA.

2.3.2 SCI shall never be handled, processed, discussed, or stored in any facility other than a properly accredited SCIF unless written authorization is granted by the CSA.

2.3.3 An inspection of the SCIF shall be performed by the CSA or appointed representative prior to accreditation. Periodic re-inspections shall be based on threat, physical modifications, sensitivity of programs, and past security performance. Inspections may occur at any time, announced or unannounced. The completed fixed facility checklist will be reviewed during the inspection to ensure continued compliance. TSCM evaluations may be required at the discretion of the CSA, as conditions warrant. Inspection reports shall be retained within the SCIF and by the CSA. All SCIFs shall maintain on site, current copies of the following documents:

- (a) DCID 1/21 Fixed Facility Checklist
- (b) Accreditation authorization documents (e.g., physical, TEMPEST, and AIS).
- (c) Inspection reports, including TSCM reports, for the entire period of SCIF accreditation.
- (d) Operating procedures, Special Security Officer/Contractor Special Security Officer (SSO/CSSO) appointment letters, Memoranda of Agreement (MOAs), Emergency Action Plans, etc.
- (e) Copies of any waivers granted by the CSA.

2.3.4 Inspection: Authorized inspectors shall be admitted to a SCIF without delay or hindrance when inspection personnel are properly certified to have the appropriate level of security clearance and SCI indoctrination for the security level of the SCIF. Short notice or emergency conditions may warrant entry without regard to the normal SCIF duty hours. Government owned equipment needed to conduct SCIF inspections will be admitted into SCIF without delay.

2.3.5 Facilities which are presently accredited, under construction or in the approval process at the date of implementation of this Manual shall not require modification to conform to these standards.

2.3.5.1 Facilities undergoing major modification may be required to comply entirely with the provisions of this Manual. Approval for such modifications shall be requested through the CSA and received prior to any modifications taking place within the SCIF.

2.3.5.2 In the event a need arises to reopen a SCIF after the accreditation has been terminated, the CSA may approve the use of a previously accredited SCIF based upon a review of an updated facility accreditation package.

2.3.6 Withdrawal of Accreditation:

2.3.6.1 Termination of Accreditation: When it has been determined that a SCIF is no longer required, withdrawal of accreditation action will be initiated by the SSO/CSSO. Upon notification, the CSA will issue appropriate SCI withdrawal correspondence. The CSA or appointed representative will conduct a close out inspection of the facility to ensure that all SCI material has been removed.

2.3.6.2 Suspension or Revocation of Accreditation: When the CSA determines that there is a danger of classified information being compromised or that security conditions in a SCIF are unsatisfactory, SCI accreditation will be suspended or revoked. All appropriate authorities must be notified of such action immediately.

2.4 Co-Utilization

2.4.1 Agencies desiring to co-utilize a SCIF should accept the current accreditation and any waivers. Any security enhancements required by an agency or department requesting co-utilization should be funded by that organization, and must be approved by the SOIC with DCI concurrence prior to implementation. A co-utilization agreement must be established prior to occupancy.

2.4.2 Special Access Programs (SAP) co-located within a SCIF will meet the physical security requirements of this Manual and DCI Special Access Programs (SAP) Policy, January 4, 1989.

2.5 Personnel Controls

2.5.1 Access rosters listing all persons authorized access to the facility shall be maintained at the SCIF point of entry. Electronic systems, including coded security identification cards or badges may be used in lieu of security access rosters.

2.5.2 Visitor identification and control: Each SCIF shall have procedures for identification and control of visitors seeking access to the SCIF.

2.6 Control of Combinations

2.6.1 Combinations to locks installed on security containers/safes, perimeter doors, windows and any other openings should be changed whenever:

- (a) A combination lock is first installed or used;
- (b) A combination has been subjected, or believed to have been subjected to compromise; and
- (c) At other times when considered necessary by the CSA.

2.6.2 All combinations to SCIF entrance doors should be stored in another SCIF of equal or higher accreditation level. When this is not feasible, alternate arrangements will be made in coordination with the CSA.

2.7 Entry/Exit Inspections

The CSA shall prescribe procedures for inspecting persons, their property, and vehicles at the entry or exit points of SCIFs, or at other designated points of entry to the building, facility, or compound. The purpose of the inspection is to deter the unauthorized removal of classified material, and deter the introduction of prohibited items or contraband. This shall include determination of whether inspections are randomly conducted or mandatory for all, and whether they apply for visitors only or for the entire staff assigned. All personnel inspection procedures should be reviewed by the facility's legal counsel prior to promulgation.

2.8 Control of Electronic Devices and Other Items

2.8.1 The CSA shall ensure that procedures are instituted for control of electronic devices and other items introduced into or removed from the SCIF. See Annex D for guidance.

2.8.2 The prohibition against electronic equipment in SCIFs does not apply to those needed by the disabled or for medical or health reasons (e.g. motorized wheelchairs, hearing aids, heart pacemakers, amplified telephone headsets, teletypewriters for the hearing impaired). However, the SSO or CSSO shall establish procedures for notification that such equipment is being entered into the SCIF.

2.8.3 Emergency and police personnel and their equipment, including devices carried by emergency medical personnel responding to a medical crisis within a SCIF, shall be admitted to the SCIF without regard to their security clearance status. Emergency personnel will be escorted to the degree practical. However, debriefing of emergency personnel will be accomplished as soon as possible, if appropriate.

2.8.4 Equipment for TEMPEST or Technical Surveillance Countermeasures (TSCM) testing shall be admitted to a SCIF as long as the personnel operating the equipment are certified to have the appropriate level of security clearance and SCI indoctrination.

3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SCIFs

3.1 Construction Policy for SCI Facilities

Physical security criteria is governed by whether the SCIF is located in the US or not, according to the following conditions: closed storage, open storage, continuous operations, secure working areas.

3.1.1. Closed Storage

3.1.1.1 Inside U.S:

- (a) The SCIF must meet the specifications in Chapter 4 (Permanent Dry Wall Construction).
- (b) The SCIF must be alarmed in accordance with Annex B to this manual.
- (c) SCI must be stored in GSA approved security containers.
- (d) There must be a response force capable of responding to an alarm within 15 minutes after annunciation and a reserve response force available to assist the responding force.
- (e) The CSA may require any SCIF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by Chapter 4 (Expanded Metal) construction requirement.

3.1.1.2. Outside U.S:

- (a) The SCIF must meet the construction specifications for SCIFs as set forth in Chapter 4 (Steel Plate or Expanded Metal). SCIFs within US Government controlled compounds¹, or equivalent, having armed immediate response forces may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction) with prior approval of the CSA.
- (b) The SCIF must be alarmed in accordance with Annex B.
- (c) All SCI controlled material will be stored in GSA-approved containers having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.
- (d) There must be a response force capable of responding to an alarm within 10 minutes and a reserve response force available to assist the responding force.

¹A controlled building or compound is one to which access is restricted and unescorted entry is limited to authorized personnel.

3.1.2. Open Storage

3.1.2.1 INSIDE US: When open storage is justified and approved by the CSA, the SCIF must:

- (a) be alarmed in accordance with Annex B;
- (b) have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the response force; and
- (c) meet one of the following:
 - (1) SCIFs within a controlled US government compound or equivalent may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction); or
 - (2) SCIFs within a controlled building with continuous personnel access control, may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction). The CSA may require any SCIF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by Chapter 4 (Expanded Metal) construction requirements; or
 - (3) SCIFs which are not located in a controlled building or compound may use specifications indicated in Chapter 4 (expanded Metal) or (Vault) constructions requirements.

3.1.2.2 OUTSIDE US: Open storage of SCI material will be avoided. When open storage is justified as mission essential, vault construction is preferred. The SCIF must:

- (a) be alarmed in accordance with Annex B;
- (b) have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.
- (c) have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster; and
- (d) meet one of the following:
 - (1) The construction specification for vaults set forth in Chapter 4 (Vaults); or
 - (2) With the approval of the CSA, SCIFs located on a controlled US government compound or equivalent having immediate response forces, may use expanded metal, steel plate, or GSA approved modular vaults in lieu of vault construction.

3.1.3 Continuous Operation

3.1.3.1 INSIDE THE US:

- (a) The SCIF must meet the construction specifications as identified in Chapter 4 (Permanent Dry Wall Construction). An alert system and duress alarm may be required by the CSA, based on operational and threat conditions.
- (b) Provisions should be made for storage of SCI in GSA approved containers. If the configuration of the material precludes this, there must be an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency, civil unrest or natural disaster.
- (c) There must be a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force.

3.1.3.2 OUTSIDE THE US:

- (a) The SCIF must meet the construction specifications for SCIFs as set forth in Chapter 4 (Expanded Metal). An alert system and duress alarm may be required by the CSA, based on operational and threat conditions. (b) The capability must exist for storage of all SCI in GSA-approved security containers, or the SCIF must have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster.
- (b) SCIFs located within US Government controlled compounds, or equivalent, having immediate response forces, may use the secure area construction specifications as listed in Chapter 4 (Permanent Dry Wall Construction) with prior approval of the CSA.
- (c) There must be a response force capable of responding to an alarm within 5 minutes, and a reserve response force available to assist the responding force.

3.1.4 Secure Working Areas are accredited facilities used for handling, discussing, and/or processing SCI, but where SCI will not be stored.

3.1.4.1 INSIDE THE US:

- (a) The Secure Working Area SCIF must meet the specifications set forth in Chapter 4 (Permanent Dry Wall Construction).
- (b) The Secure Working Area SCIF must be alarmed with a balanced magnetic switch on all perimeter entrance doors.
- (c) No storage of SCI material is authorized.

UNCLASSIFIED

- (d) There must be a response force capable of responding to an alarm within 15 minutes after annunciation, and a reserve response force available to assist the responding force.

3.1.4.2 OUTSIDE THE US:

- (a) The Secure Working Area SCIF must meet the construction specifications indicated in Chapter 4 (Permanent Dry Wall Construction).
- (b) The Secure Working Area SCIF must be equipped with an approved alarm system as set forth in Annex B.
- (c) No storage of SCI material is authorized.
- (d) There must be a response force capable of responding to an alarm within 10 minutes, and a reserve response force available to assist the responding force.

3.2 Temporary Secure Working Area (TSWA)

3.2.1 A Temporary Secure Working area is defined as a temporarily accredited facility that is used no more than 40 hours monthly for the handling, discussion, and/or processing of SCI, but where SCI should not be stored. With sufficient justification, the CSA may approve longer periods of usage and storage of SCI for no longer than 6 months.

3.2.2 During the entire period the TSWA is in use, the entrance will be controlled and access limited to persons having clearance for which the area has been approved. Approval for using such areas must be obtained from the CSA setting forth room number(s), building, location, purpose, and specific security measures employed during usage as well as during other periods. TSWAs should be covered by an alarm system. These areas should not be used for periods exceeding an average total of 40 hours per month. No special construction is required other than to meet sound attenuation requirements as set forth in Annex E, when applicable. If such a facility must also be used for the discussion of SCI, a Technical Surveillance Countermeasures (TSCM) evaluation may be required at the discretion of the CSA, as conditions warrant.

3.2.3 When not in use at the SCI level, the TSWA will be:

- (a) Secured with a keylock or a combination lock approved by the CSA.
- (b) Access will be limited to personnel possessing a US Secret clearance.

3.2.4 If such a facility is not alarmed or properly protected during periods of non-use, a TSCM inspection may be conducted prior to use for discussion at the SCI level.

3.3 Requirements Common To All SCIFs; Within The US and Overseas

3.3.1 **CONSTRUCTION:** The SCIF perimeter walls, floors and ceiling, will be permanently constructed and attached to each other. All construction must be done in such a manner as to provide visual evidence of unauthorized penetration.

3.3.2 **SOUND ATTENUATION:** The SCIF perimeter walls, doors, windows, floors and ceiling, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of conversation. The requirements for sound attenuation are contained within Annex E.

3.3.3 ENTRANCE, EXIT, AND ACCESS DOORS:

3.3.3.1 Primary entrance doors to SCIFs shall be limited to one. If circumstances require more than one entrance door, this must be approved by the CSA. In some circumstances, an emergency exit door may be required. In cases where local fire regulations are more stringent, they will be complied with. All perimeter SCIF doors must be closed when not in use, with the exception of emergency circumstances. If a door must be left open for any length of time due to an emergency or other reasons, then it must be controlled in order to prevent unauthorized removal of SCI.

3.3.3.2 All SCIF perimeter doors must be plumbed in their frames and the frame firmly affixed to the surrounding wall. Door frames must be of sufficient strength to preclude distortion that could cause improper alignment of door alarm sensors, improper door closure or degradation of audio security.

3.3.3.3 All SCIF primary entrance doors must be equipped with an automatic door closer, a GSA-approved combination lock and an access control device with the following requirements:²

(a) If doors are equipped with hinge pins located on the exterior side of the door where it opens into an uncontrolled area outside the SCIF, the hinges will be treated to prevent removal of the door (e.g. welded, set screws, etc.)

(b) If a SCIF entrance door is not used as an access control door and stands open in an uncontrolled area, the combination lock will be protected against unauthorized access/tampering.

3.3.3.4 **Control doors:** The use of a vault door for controlling daytime access to a facility is not authorized. Such use will eventually weaken the locking mechanism, cause malfunctioning of the emergency escape device, and constitute a security and safety hazard. To preclude this, a second door will be installed and equipped with an automatic door closer and an access control device. (It is preferable that the access door be installed external to the vault door.)

²This requirement does not apply to the GSA approved Class 5,6, and 8 vault doors.

3.3.3.5 SCIF emergency exit doors shall be constructed of material equivalent in strength and density to the main entrance door. The door will be secured with deadlocking panic hardware on the inside and have no exterior hardware. SCIF perimeter emergency exit doors should be equipped with a local annunciator in order to alert people working in the area that someone exited the facility due to some type of emergency condition.

3.3.3.6 Door Construction Types: Selections of entrance and emergency exit doors shall be consistent with SCIF perimeter wall construction. Specifications of doors, combination locks, access control devices and other related hardware may be obtained from the CSA. Some acceptable types of doors are:

- (a) Solid wood core door, a minimum of 1 3/4 inches thick.
- (b) Sixteen gauge metal cladding over wood or composition materials, a minimum of 1 3/4 inches thick. The metal cladding shall be continuous and cover the entire front and back surface of the door.
- (c) Metal fire or acoustical protection doors, a minimum of 1 3/4 inches thick. A foreign manufactured equivalent may be used if approved by the CSA.
- (d) A joined metal rolling door, minimum of 22 gauge, used as a loading dock or garage structure must be approved on a case-by-case basis.

3.3.4 PHYSICAL PROTECTION OF VENTS, DUCTS, AND PIPES:

3.3.4.1 All vents, ducts, and similar openings in excess of 96 square inches that enter or pass through a SCIF must be protected with either bars, or grills, or commercial metal duct sound baffles that meet appropriate sound attenuation class as specified in Annex E. Within the United States, bars or grills are not required if an IDS is used. If one dimension of the duct measures less than six inches, or duct is less than 96 square inches, bars are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch diameter steel welded vertically and horizontally six (6) inches on center; if grills are used, they must be of 9-gauge expanded steel; if commercial sound baffles are used, the baffles or wave forms must be metal permanently installed and no farther apart than six (6) inches in one dimension. A deviation of 1/2 inch in vertical and/or horizontal spacing is permissible.

3.3.4.2 Based on the TEMPEST accreditation, it may be required that all vents, ducts, and pipes must have a non-conductive section (a piece of dissimilar material e.g., canvas, rubber) which is unable to carry electric current, installed at the interior perimeter of the SCIF.

3.3.4.3 An access port to allow visual inspection of the protection in the vent or duct should be installed inside the secure perimeter of the SCIF. If the inspection port must be installed outside the perimeter of the SCIF, it must be locked.

3.3.5 WINDOWS:

3.3.5.1 All windows which might reasonably afford visual surveillance of personnel, documents, materials, or activities within the facility, shall be made opaque or equipped with blinds, drapes or other coverings to preclude such visual surveillance.

3.3.5.2 Windows at ground level³ will be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. SCIFs located within fenced and guarded government compounds or equivalent may eliminate this requirement if the windows are made inoperable by either permanently sealing them or equipping them on the inside with a locking mechanism.

3.3.5.3 All perimeter windows at ground level shall be covered by an IDS.

4. CONSTRUCTION SPECIFICATIONS

4.1 Vault Construction Criteria

4.1.1 Reinforced Concrete Construction: Walls, floor, and ceiling will be a minimum thickness of eight inches of reinforced concrete. The concrete mixture will have a comprehensive strength rating of at least 2,500 psi. Reinforcing will be accomplished with steel reinforcing rods, a minimum of 5/8 inches in diameter, positioned centralized in the concrete pour and spaced horizontally and vertically six inches on center; rods will be tied or welded at the intersections. The reinforcing is to be anchored into the ceiling and floor to a minimum depth of one-half the thickness of the adjoining member.

4.1.2 GSA-approved modular vaults meeting Federal Specification FF-V-2737, may be used in lieu of a 4.1.1. above.

4.1.3 Steel-lined Construction: Where unique structural circumstances do not permit construction of a concrete vault, construction will be of steel alloy-type of 1/4" thick, having characteristics of high yield and tensile strength. The metal plates are to be continuously welded to load-bearing steel members of a thickness equal to that of the plates. If the load-bearing steel members are being placed in a continuous floor and ceiling of reinforced concrete, they

³This should be interpreted to mean any windows which are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, (e.g. electrical transformer, air conditioning units, vegetation, or landscaping which can easily be climbed, etc.).

must be firmly affixed to a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than six inches of reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

- 4.1.4 All vaults shall be equipped with a GSA-approved Class 5 or Class 8 vault door. Within the US, a Class 6 vault door is acceptable. Normally within the United States a vault will have only one door that serves as both entrance and exit from the SCIF in order to reduce costs.

4.2 SCIF Criteria For Permanent Dry Wall Construction

Walls, floor and ceiling will be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, must be done in such a manner as to provide visual evidence of unauthorized penetration.

4.3 SCIF Construction Criteria For Steel Plate

Walls, ceiling and floors are to be reinforced on the inside with steel plate not less than 1/8" thick. The plates at all vertical joints are to be affixed to vertical steel members of a thickness not less than that of the plates. The vertical plates will be spot welded to the vertical members by applying a one inch long weld every 12 inches; meeting of the plates in the horizontal plane will be continuously welded. Floor and ceiling reinforcements must be securely affixed to the walls with steel angles welded or bolted in place.

4.4 SCIF Construction Criteria For Expanded Metal

Walls are to be reinforced, slab to slab, with 9-gauge expanded metal. The expanded metal will be spot welded every 6 inches to vertical and horizontal metal supports of 16-gauge or greater thickness that has been solidly and permanently attached to the true floor and true ceiling.

4.5 General

The use of materials having thickness or diameters larger than those specified above is permissible. The terms "anchored to and/or embedded into the floor and ceiling" may apply to the affixing of supporting members and reinforcing to true slab or the most solid surfaces; however, subfloors and false ceiling are not to be used for this purpose.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

GLOSSARY:

Access Control System:	A system to identify and/or admit personnel with properly authorized access to a SCIF using physical, electronic, and/or human controls.
Accreditation:	The formal approval of a specific place, referred to as a Sensitive Compartmented Information Facility(SCIF), that meets prescribed physical, technical, and personnel security standards.
Acoustic Security:	Those security measures designed and used to deny aural access to classified information.
Astragal Strip:	A narrow strip of material applied over the gap between a pair of doors for protection from unauthorized entry and sound attenuation.
Authorized Personnel:	A person who is fully cleared and indoctrinated for SCI, has a valid need to know, and has been granted access to the SCIF.
Balanced Magnetic Switch (BMS):	A type of IDS sensor which may be installed on any rigid, operable opening (i.e. doors, windows) through which access may be gained to the SCIF.
Break-Wire Detector:	An IDS sensor used with screens and grids, open wiring, and grooved stripping in various arrays and configurations necessary to detect surreptitious and forcible penetrations of movable openings, floors, walls, ceilings, and skylights. An alarm is activated when the wire is broken.
Closed Storage:	The storage of SCI material in properly secured GSA approved security containers within an accredited SCIF.
Computerized Telephone System (CTS):	Also referred to as a hybrid key system, business communication system, or office communications system.
Cognizant Security Authority (CSA):	The single principal designated by a SOIC (see definition of SOIC) to serve as the responsible official for all aspects of security program management with respect to the protection of intelligence sources and methods, under SOIC responsibility.
Continuous Operation:	This condition exists when a SCIF is staffed 24 hours every day.
Controlled Area/Compound:	Any area to which entry is subject to restrictions or control for security reasons.
Controlled Building:	A building to which entry is subject to restrictions or control for security reasons.
Co-Utilization:	Two or more organizations sharing the same SCIF.

UNCLASSIFIED

Dead Bolt:	A lock bolt with no spring action. Activated by a key or turn knob and cannot be moved by end pressure.
Deadlocking Panic Hardware:	A panic hardware with a deadlocking latch that has a device when in the closed position resists the latch from being retracted.
Decibel (db):	A unit of sound measurement.
Document:	Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.
Dual Technology:	PIR, microwave or ultrasonic IDS sensors which combine the features of more than one volumetric technology.
Expanded Steel:	Also called EXPANDED METAL MESH. A lace work patterned material produced from sheet steel by making regular uniform cuts and then pulling it apart with uniform pressure.
Guard:	A properly trained and equipped individual whose duties include the protection of a SCIF. Guards whose duties require direct access to a SCIF, or patrol within a SCIF, must meet the clearance criteria in Director of Central Intelligence Directive 1/14. CSA will determine if indoctrination is required.
Intelligence Community (and agencies within the Intelligence Community):	Refers to the United States Government agencies and organizations identified in section 3.4(f) (1 through 7) of Executive Order 12333.
Intrusion Detection System:	A security alarm system to detect unauthorized entry.
Isolator:	A device or assembly of devices which isolates or disconnects a telephone or Computerized Telephone System (CTS) from all wires which exit the SCIF and which as been accepted as effective for security purposes by the Telephone Security Group (TSG approved).
Key Service Unit (KSU):	An electromechanical switching device which controls routing and operation of an analog telephone system.
Line Supervision:	
Class I:	Class I line security is achieved through the use of DES or an algorithm based on the cypher feedback or cypher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required.

Class II:	Class II line supervision refers to systems in which the transmission is based on pseudo random generated or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum six month period, Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.
Motion Detection Sensor:	An alarm sensor that detects movement.
Non-Conductive Section:	Material (i.e. canvas, rubber, etc.) which is installed in ducts, vents, or pipes, and is unable to carry audio or RF emanations.
Non-Discussion Area:	A clearly defined area within a SCIF where classified discussions are not authorized due to inadequate sound attenuation.
Open Storage:	The storage of SCI material within a SCIF in any configuration other than within GSA approved security containers.
Response Force:	Personnel (not including those on fixed security posts) appropriately equipped and trained, whose duties include initial or follow up response to situations which threaten the security of the SCIF. This includes local law enforcement support or other external forces as noted in agreements.
Secure Working Area:	An accredited SCIF used for handling, discussing and/or processing of SCI, but where SCI will not be stored.
Senior Official of the Intelligence Community (SOIC):	The head of an agency, office, bureau, or intelligence element identified in section 3.4(f) (1 through 6) of Executive Order 12333.
Sensitive Compartmented Information (SCI):	SCI is classified information concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.
Sensitive Compartmented Information Facility (SCIF):	An accredited area, room, group of rooms, building, or installation where SCI may be stored, used, discussed and/or electronically processed.
Sound Group:	Voice transmission attenuation groups established to satisfy acoustical requirements. Ratings measured in sound transmission class may be found in the Architectural Graphic Standards.
Sound Transmission Class (STC):	The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.
Special Access Program (SAP):	Any approved program which imposes need-to-know or access controls beyond those normally required for access to CONFIDENTIAL, SECRET or TOP SECRET information.

UNCLASSIFIED

Surreptitious Entry: Unauthorized entry in a manner which leaves no readily discernible evidence.

Tactical SCIF: An accredited area used for actual or simulated war operations for a specified period of time.

Technical Surveillance Countermeasures (TSCM) Surveys and Evaluations: A physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration.

Type Accepted Telephone: Any telephone whose design and construction conforms with the design standards for Telephone Security Group approved telephone sets. (TSG Standard #3, #4, or #5).

Vault: A room(s) used for the storing, handling, discussing, and/or processing of SCI and constructed to afford maximum protection against unauthorized entry.

Waiver: An exemption from a specific requirement of this document.

UNCLASSIFIED

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

ANNEX A
(Effective 27 May 1994)

SCIF ACCREDITATION CHECKLIST

Table of Contents

Section A — General Information	3
Section B — Peripheral Security	5
Section C — SCIF Security	5
Section D — Doors	7
Section E — Intrusion Detection Systems	8
Section F — Telephone System	9
Section G — Acoustical Protection	10
Section H — Administrative Security	11
Attachments	

DATE _____

FIXED FACILITY CHECKLIST

[] PRECONSTRUCTION [] NEW [] MODIFIED FACILITY

Section A — General Information

1. SCIF Data: Organization/Company Name: _____
SCIF Identification Number (if applicable): _____
Organization subordinate to (If applicable): _____
Contract Number & Expiration Date: _____
CSA: _____
Project Headquarter Security Office (if applicable): _____

2. SCIF Location:
Street Address: _____
Bldg Name/#: _____ Floor: _____
Room(s) No: _____
City: _____ State/Country: _____
ZIP Code: _____

3. Responsible Security Personnel:
Primary: _____ Alternate: _____
Commercial Telephone: _____
DSN Telephone: _____
Secure Telephone: Type: _____
Home Telephone: _____
Fax No: (specify both classified and unclassified)
Classified: _____ Unclassified: _____
Other: _____

4. Accreditation Data:

a. Category of SCI Requested: _____

Indicate the storage required: Open Storage Closed Storage Continuous Operation Secure Working Area Temporary Secure Working Area

b. Existing Accreditation Information (If applicable):

(1) Category of SCI: _____

(2) Accreditation granted by: _____
on _____

c. Last TEMPEST Accreditation (if applicable): Accreditation granted by: _____ on _____

d. If Automated Information Systems (AISs) are used, has an accreditation been granted? YES NO

Accreditation granted by: _____ on _____

e. SAP co-located within SCIF? YES NO
(If Yes, Classification: _____, and provide copy of Co-utilization Agreement for SAP operation in SCIF.)

f. Duty Hours: _____ hours to _____ hours, _____ days per week.

g. Total square feet SCIF occupies: _____

5. Construction/modification: Is construction or modification complete?
 YES NO N/A (If NO, expected date of completion) _____

6. Inspections:

a. TSCM Service completed by _____ on _____
(Attach copy of report)

Were deficiencies corrected? YES NO NA (If NO, explain:) _____

b. Last Physical Security Inspection by _____ on _____
(Attach copy of report)

Were deficiencies corrected? YES NO NA (If NO, explain:) _____

c. Last Security/Assistance Visit by _____ on _____

7. REMARKS: _____

Section B — Peripheral Security

8. Describe building exterior security:
- a. Fence: _____
 - b. Fence Alarm: _____
 - c. Fence lighting: _____
 - d. Television (CCTV): _____
 - e. Guards: _____
 - f. Other: _____

9. Building:
- a. Construction type: _____
 - b. Describe Access Controls: _____
 - (1) Continuous: ___ YES ___ NO
 - (2) If NO, during what hours? _____

10. Remarks: _____

Section C — SCIF Security

11. How is access to the SCIF controlled?
- a. By Guard Force: ___ YES ___ NO Security Clearance Level: _____
 - b. By Assigned Personnel: ___ YES ___ NO
 - c. By Access Control Device: ___ YES ___ NO
If yes, Manufacturer _____ Model No _____
12. Does the SCIF have windows? ___ YES ___ NO
- a. How are they acoustically protected? (If applicable) _____

b. How are they secured against opening? _____

c. How are they protected against visual surveillance? (If applicable) _____

13. Do ventilation ducts penetrate the SCIF perimeter? ____ YES ____ NO

a. Number and size (Indicate on floor plan): _____

b. If over 96 square inches, type of protection used:

(1) IDS: ____ YES ____ NO (Describe in Section E)

(2) Bars/Grills/Metal Baffles: ____ YES ____ NO
____ OTHER - Explain: _____

c. Metal Duct Sound Baffles: Are ducts equipped with:

(1) Metal Baffles: ____ YES ____ NO

(2) Noise Generator: ____ YES ____ NO

(3) Non-Conductive Joints: ____ YES ____ NO

(4) Inspection Ports: ____ YES ____ NO

If YES, are they within the SCIF? YES ____ NO ____ If they are located outside of the SCIF, how are they secured? _____

d. If TEMPEST accreditation authority requires; are pipes, conduits, etc., penetrating the SCIF equipped with non-conductive unions at the point they breach the SCIF perimeter?
____ YES ____ NO

Are they provided acoustical protection? (if applicable) ____ YES ____ NO

14. Construction:

a. Perimeter walls:

(1) Material & Thickness: _____

(2) Do the walls extend from the true floor to the true ceiling? ____ YES ____ NO

b. True ceiling (material and thickness): _____

c. False ceiling? ____ YES ____ NO If yes:

(1) Type of ceiling material: _____

(2) Distance between false and true ceiling: _____

d. True floor (material and thickness): _____

e. False Floor? YES NO If yes:
Distance between false and true floor: _____

15. Remarks: _____

Section D — Doors

16. Describe SCIF Primary Entrance Door (Indicate on floor plan): _____

Is an automatic door closer installed? YES NO If NO, explain: _____

17. Describe number and type of doors used for SCIF emergency exits and other perimeter doors
(Indicate on floor plan): _____

Is an automatic door closer installed? YES NO If NO, explain: _____

18. Describe how the door hinges exterior to the SCIF are secured against removal (if in an
uncontrolled area): _____

19. Locking devices:

a. Perimeter SCIF Entrance Door:

(1) List manufacturer, model number and Group rating: _____

(2) Does entrance door stand open into an uncontrolled area?
 YES NO If YES, describe tamper protection: _____

b. Emergency Exits and Other Perimeter Doors:

Describe (locks, metal strip/bar, deadbolts, panic hardware): _____

c. Where are the door lock combinations filed? _____

20. Remarks: _____

Section E — Intrusion Detection Systems

Give manufacturer and model numbers in response to following questions:

21. Method of Interior Motion Detection Protection:

- a. Accessible Perimeter? _____
Storage Areas? _____
- b. Motion Detection Sensors (Indicate on floor Plan): _____
Tamper protection: ___ YES ___ NO
- c. Other (e.g. CCTV, etc.): _____

22. Door and Window Protection (Indicate on floor plan):

- a. Balanced Magnetic Switch (BMS) on door?: _____
Tamper protection: ___ YES ___ NO
- b. If SCIF has ground floor windows, how are they protected? _____
- c. Other (e.g. CCTV, etc..) _____

23. Method of ventilation and duct work protection: _____

24. Space above false ceiling (only outside the United States, if required):

- a. Motion Detection Sensors: _____
Tamper protection: ___ YES ___ NO
- b. Other (e.g. CCTV): _____

25. Space below false floor (only outside the United States, if required):

- a. Motion Detection Sensors: _____
Tamper protection: ___ YES ___ NO
- b. Other (e.g. CCTV): _____

26. IDS transmission line security protection:

- a. Electronic line supervision (Manufacture and Model): _____

If electronic line supervision, class of service: ___ I ___ II

- b. Other: _____
- 27. Is emergency power available for the IDS? ___ YES ___ NO
TYPE: ___ Battery ___ Emergency Generator ___ Other
- 28. Where is the IDS control unit for the SCIF located (Indicated on floor plan)? _____

- 29. Where is the IDS Alarm annunciator panel located (Indicate on floor plan, Address)? _____

- 30. IDS Response Personnel: Describe: _____

Response Force Security Cleared: ___ YES ___ NO

Level: _____

- b. Emergency Procedures documented? ___ YES ___ NO
- c. Reserve Force available? ___ YES ___ NO
- d. Response time required for alarm condition: _____ minutes.
- e. Are response procedures tested and records maintained? ___ YES ___ NO
If no, explain: _____
- 31. Is the IDS tested and records maintained? ___ YES ___ NO
If no, explain: _____
- 32. Remarks: _____

Section F — Telephone System

- 33. Method of on-hook security provided:
 - a. TSG-2 Computerized Telephone System (CTS)? YES NO
 - (1) Manufacturer/Model: _____
 - (2) Location of the CTS: _____
 - (3) Do the CTS installers and programmers have security clearances? _____
If yes, at what access level (minimum established by CSA): _____

 - If no, are escorts provided? _____

- (4) Is the CTS installed as per TSG-2 Configuration Requirements? YES NO
- (a) If no, provide make and model number of telephone equipment, explain your configuration, and attach a line drawing? _____
- (b) Is access to the facility housing the switch controlled? YES NO
- (c) Are all lines between the SCIF and the switch in controlled spaces?
 YES NO
- (5) Does the CTS use remote maintenance and diagnostic procedures or other remote access features? YES NO
- If yes, explain those procedures: _____

b. TSG-6 approved telephones?

- (1) Manufacturer/Model: _____
- (2) TSG number: _____
- (3) Ringer Protection (if required): _____

c. TSG-6 approved disconnect devices?

- (1) Manufacturer/Model: _____
- (2) TSG number: _____

34. Methods of off-hook security provided:

- a. Is there a hold or mute feature? YES NO
- (1) If yes, which feature _____, and is it provided by the: CTS?
or Telephone
- (2) If no, are approved push-to-operated handsets provided? YES NO
Describe: _____

35. Automatic telephone call answering:

- a. Is there an automatic call answering service for the telephones in the SCIF?
 YES NO
- If yes, provide make and model number of the equipment, explain the configuration, and provide a line drawing. _____

Section G — Acoustical Protection

40. Do all areas of the SCIF meet acoustical requirements? Yes No

If no, describe additional measures taken to provide minimum acoustical protection (e.g. door, windows, etc) _____

41. Is the SCIF equipped with a public address, emergency/fire announcement or music system?
___ Yes ___ No

If yes, describe and explain how protected? _____

42. If any intercommunication system that is not part of the telephone system is used, describe and explain how protected: _____

43. Remarks: _____

Section H — Administrative Security

45. Destruction Methods:

a. Describe method used for destruction of classified/sensitive material:

Manufacturer: _____ Model: _____
Manufacturer: _____ Model: _____

b. Describe location of destruction site(s) in relation to the secure facility: _____

c. Have provisions been made for the emergency destruction of classified/sensitive program material? (If required): ___ YES ___ NO

If YES, has the emergency destruction equipment and plan been coordinated with the CSA?
___ YES ___ NO

46. If reproduction of classified/sensitive material takes place outside the SCIF, describe equipment and security procedures used to reproduce documents: _____

47. Remarks: _____

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

ANNEX B
(Effective 27 May 1994)

INTRUSION DETECTION SYSTEMS

Annex B sets forth the requirements and establishes the standards for intrusion detection systems for all SCIFs throughout government and for government-sponsored contractor facilities. Compliance with these standards is mandatory for all facilities established after the effective date of this annex, including any major renovation of existing facilities insofar as the renovation will permit reasonable and practical upgrading, as determined by the Cognizant Security Authority (CSA).

1.0 CONCEPT

An Intrusion Detection System (IDS) must detect an attempted or actual human entry into the protected area. An IDS complements other physical security measures and consists of three essential components:

- 1.1 Intrusion Detection Equipment (IDE).
- 1.2 Security and response force personnel.
- 1.3 Operation procedures.

2.0 OPERATION

- 2.1 IDS components operate as a system with four distinct phases:
 - 2.1.1 Detection.
 - 2.1.2 Reporting.
 - 2.1.3 Assessment.
 - 2.1.4 Response.
- 2.2 These elements are equally important, and none can be eliminated if an IDS is to provide an acceptable degree of protection.
 - 2.2.1 Detection: The detection phase begins as soon as a detector or sensor reacts to stimuli it is designed to detect. The sensor alarm condition is then transmitted over cabling located within the protected area to the Premise Control Unit (PCU). The PCU may service many sensors. The PCU and the sensors it serves comprise a "zone" at the monitor station. This shall be used as the definition of an alarmed zone for purposes of this document.
 - 2.2.2 Reporting: The PCU receives signals from all sensors in a protected area and incorporates these signals into a communication scheme. Another signal is added to the communication for supervision to prevent compromise of the communications scheme. This supervised signal is intended to disguise the

information and protect the IDS against tampering or injection of false information by an intruder. The supervised signal is sent by the PCU via the transmission link to the monitor station. Inside the monitor station, either a dedicated panel or central processor monitors information from the PCU signals. When alarms occur, an annunciator generates an audible and visible alert to security personnel. Alarms result normally from intrusion, tampering, component failure, or system power failure.

2.2.3 **Assessment:** The assessment period is the first phase that requires human interaction. When alarm conditions occur, the operator assesses the situation and dispatches the response force.

2.2.4 **Response:** The response phase begins as soon as the operator assesses an alarm condition. A response force must immediately respond to all alarms. The response phase must also determine the precise nature of the alarm and take all measures necessary to safeguard the SCIF.

3.0 REQUIREMENTS

3.1 As determined by the CSA, all areas of a SCIF that reasonably afford access to the SCIF, or where SCI is stored, shall be protected by an IDS unless continually occupied.

3.2 **Acceptability of Equipment:** All IDE must be UL-listed (or equivalent as defined by the CSA) and approved by the CSA. Government and proprietary installed, maintained, or furnished systems are subject to approval only by the CSA.

3.3 **Vendor Approval Procedures:** Vendors may submit their IDE requests either through a Special Security Officer/Contractor Special Security Officer (SSO/CSSO) or directly to the CSA. Vendors should provide a UL certificate for installation and service (UL 611, 681, 1076, and 2050 apply) directly to the SSO/CSSO or CSA for acceptance. With sufficient justification, the CSA may waive this requirement and waivers must be documented. All requests for acceptance must describe the IDE fully and include the results of testing by a listed independent laboratory. An independent laboratory evaluates the manufacturer's compliance to performance specifications. A request for acceptance of line supervision using Data Encryption Standard (DES) must also include validation from the National Institute of Standards and Technology (NIST) or another independent testing laboratory recognized by the CSA. The description must identify the manufacturer and model of equipment and show how the IDE meets CSA and/or UL standards.

3.4 **Preinstallation Approval of IDS:** The CSA will approve a proposed IDS before its installation within a SCIF as part of the initial SCIF construction approval process. A proposal for an IDS will be examined for the type and employment of accepted equipment. An IDS proposal will be submitted as part of a preconstruction approval process.

3.5 **Equipment:**

3.5.1 **Transmission Line Security:** When the transmission line leaves the SCIF and traverses an uncontrolled area, Class I or Class II CSA accepted line security shall be used.

- 3.5.1.1 Class I: Class I line security is achieved through the use of DES or an algorithm based on the cipher feedback or cipher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required. The certificate must be retained by the CSA for the duration of operation of the SCIF.
- 3.5.1.2 Class II: Class II line supervision refers to systems in which the transmission is based on pseudo-random generated tones or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum six-month period. Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.
- 3.5.2 Internal Cabling: The cabling between the sensors and the PCU should be dedicated to IDE and must comply with national and local code standards. If applicable, the cabling must be installed in accordance with TEMPEST and COMSEC requirements.
- 3.5.3 Restriction on Integration of Access Controls into SCIF IDSs: If an access control system is integrated into an IDS, reports from the access control system should be subordinate in priority to reports from intrusion alarms.
- 3.5.4 Maintenance Mode: When an alarm zone is placed in the maintenance mode, this condition will be signaled automatically to the monitor station. This signal must appear as an alarm or maintenance message at the monitor station, and the IDS shall not be securable while in the maintenance mode. However, the alarm or message must continue visibly at the monitor station throughout the period of maintenance. A standard operating procedure (SOP) must be established to address appropriate actions when maintenance access is indicated at the panel. All maintenance periods will be archived in the system. The CSA may require that the maintenance Personal Identification Number (PIN) be established and controlled by the customer. The IDE will not contain any capability for remote diagnostics, maintenance, or programming, except for an alarm remote test feature at the monitor station. A self-test feature will be limited to one second per occurrence.
- 3.5.5 Annunciation of Shunting or Masking Condition: Shunting or masking of any internal zone or sensor must be appropriately logged or recorded in archive. A shunted or masked internal zone or sensor must be displayed as such at the monitor station throughout the period the condition exists whenever there is a survey of zones or sensors.
- 3.5.6 Alarms Indications: Indications of alarm status shall be revealed at the monitoring station and optionally within the confines of the SCIF.
- 3.5.7 Power Supplies: Primary power for all IDE will be commercial AC or DC power. In the event of commercial power failure at the protected area or monitor station, the equipment will change power sources without causing an alarm indication.

- 3.5.7.1 **Emergency Power:** Emergency power must comply with UL 603. Emergency power may consist of battery and/or generator power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. The manufacturer's periodic maintenance schedule shall be followed and results documented.
- 3.5.7.2 **Power Source and Failure Indication:** An illuminated indication will exist at the PCU of the power source in use (AC or DC). Equipment at the monitor station will indicate visibly and audibly a failure in power source, a change in power source, and the location of the failure or change.
- 3.5.8 **Tamper Protection:** All IDE within the SCIF with removable covers will be equipped with tamper switches. The tamper detection will be monitored continuously whether the IDS is in the access or secure mode of operation.
- 3.5.9 **Prohibition Against Fortuitous Conduction via IDE:** No IDE will be employed that allows audio and intelligence-bearing signals to pass out of the SCIF in any form.
- 3.5.10 **Safeguarding IDE:**
 - 3.5.10.1 **In areas outside the United States, IDE must remain solely under US control, or as otherwise authorized by the CSA.**
 - 3.5.10.2 **Key variables and operational passwords will be safeguarded, disseminated, and controlled as determined by the CSA.**

3.6 Installation:

- 3.6.1 **Independent Equipment:** All SCIFs will have intrusion detection equipment and zones independent from other protected sites. When many alarmed areas are protected by one monitor station, audible and visible annunciations for SCIF zones must be clearly distinguishable from other annunciations. All sensors protecting the SCIF will be installed within the SCIF.
- 3.6.2 **Access/Secure Switch and PCU:** No capability will exist to allow changing the access status of the IDS from a location outside the SCIF unless performed by a properly accessed individual. All PCUs must be located inside the SCIF and should be located near the SCIF entrance. SCIF personnel must initiate all changes in access and secure status. Operation of the PCU will be restricted by use of a device or procedure that verifies authorized use. In the secure mode, any unauthorized entry into the SCIF shall cause an alarm to be transmitted immediately to the monitor station.
- 3.6.3 **Motion Detection Protection:** All areas of the SCIF that reasonably afford access to the SCIF or where SCI is stored shall be protected with motion detection sensors, e.g., ultrasonic, passive infrared, etc. Use of dual

technology is authorized when one technology transmits an alarm condition independently from the other technology. A failed detector will cause an immediate and continuous alarm condition. Detection equipment must be installed in compliance with UL 681 and 1076.

- 3.6.4 Accessible Areas: Within the United States, alarms are not required above the false ceiling or below the false floor. Outside the United States, such alarms may be required by the CSA.
- 3.6.5 Protection of SCIF Perimeter Doors: Each SCIF perimeter door will be protected by a balanced magnetic switch (BMS) that meets the minimum standards of UL 634. The BMS must be installed in such a manner that an alarm signal will initiate before the nonhinged side of the door opens beyond the thickness of the door from the seated position. Emergency exit doors equipped with integrated life safety hardware may have the life safety alarm component integrated into the SCIF IDS as an additional detector. Emergency exit doors will be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication.
- 3.6.6 Windows: All readily accessible windows¹ will be protected by an IDS, either independently or by the motion detection sensors in the room, as determined by the CSA.
- 3.6.7 IDE Installation Criteria: All IDE will be installed in a manner to prevent access or removal from a location external to the SCIF and in compliance with UL 681 for "Installation of Burglar Alarm Equipment."
- 3.6.8 IDS Requirements for Continuous Operations Facilities: A SCIF accredited for continuous operations may not require an IDS as determined by the CSA. This type of SCIF will be equipped with an alerting system if the occupants cannot observe all potential entrances into the SCIF. The system alerts occupants to an intrusion into the SCIF. An alert system will consist of BMSs or other appropriate sensors. None of the IDE or cabling associated with the alert system will extend beyond the perimeter of the SCIF.
- 3.6.9 False/Nuisance Alarm: Any alarm signal transmitted in the absence of a detected intrusion is a false alarm. A false alarm becomes a nuisance alarm when the effects of environment, equipment malfunction, operator failure, animals, electrical disturbances, and known effects cause the alarm indication. All alarms shall be investigated and the results documented. The maintenance program for the IDS shall ensure that incidents of false/nuisance alarms will not exceed one in a period of 30 days per zone.

¹This should be interpreted to mean any windows which are less than 18 feet above the ground measured from the bottom of the window, or are easily accessible by means of objects directly beneath the windows, (e.g. electrical transformer, air conditioning units, vegetation, or landscaping which can easily be climbed, etc.).

3.7 Personnel:

- 3.7.1 IDE Installation and Maintenance Personnel: Alarm installation and maintenance will be accomplished by US citizens who have been subjected to a trustworthiness determination (e.g., NAC with no clearance to be issued). Use of foreign nationals or other personnel for this purpose must have prior CSA approval.
- 3.7.2 Monitor Station Staffing: The monitor station will be supervised continuously by US citizens who have been subjected to a trustworthiness determination (e.g., NAC with no clearance to be issued). Use of foreign nationals or other personnel for this purpose must have prior CSA approval. The duties of the monitoring operator will be documented and will entail observing monitor panels for reports of alarms and changes in IDE status, making accurate assessments of these reports, and dispatching the response force or notifying the appropriate authority in the event of an intrusion alarm. The operator will have no duties that interfere with the primary functions of monitoring alarms and dispatching the response force. A documented chain of authority will exist for use by security personnel during unusual situations. The operator will be trained sufficiently in the operation and theory of the IDE to properly interpret all incidents generated by the IDE. This training must also include all actions to be taken on receipt of an alarm activation.

3.8 Procedures:

- 3.8.1 Testing: SCIF IDS sensors will be tested semiannually. A record of IDE testing will be maintained at the SCIF that reflects: testing date, individuals who performed the test, specific equipment tested, malfunctions, and corrective actions taken. Tests of the response force will be conducted semiannually. A record of response force testing will be maintained.
- 3.8.2 Safeguarding IDS Plans: Details of installed IDS shall be controlled and restricted on a need-to-know basis.
- 3.8.3 Operating Procedures: A written support agreement must be established for external monitoring and/or response.
- 3.8.4 Monitoring Station: Where there is an operations security concern, the alarm monitoring panel shall be designed to prevent observation by unauthorized persons.
- 3.8.5 Alarm Condition Response: Every alarm condition will be treated initially as a detected intrusion until resolved by the response force. The response force will investigate the source of an alarm and will notify SCIF personnel. The response force will take appropriate steps to safeguard the SCIF and prevent the escape of an intruder from the SCIF as permitted by SOP, local law enforcement, and circumstances until properly relieved. Response time to an alarm will not exceed:
- 3.8.5.1 Open Storage Area_five minutes
 - 3.8.5.2 Closed Storage Area_15 minutes

- 3.8.6 Catastrophic Failure: If the IDE suffers catastrophic failure, or loses primary and emergency power, SCIF-indoctrinated individuals must provide security by physically occupying the SCIF until the IDS can be made functional. As an alternative, the outside SCIF perimeter may be continuously protected by the response force or as determined by the CSA.
- 3.8.7 IDS Logging: The IDS will incorporate a means for providing a historical record of all events, either automatically or through the use of a manual log system. If the IDE has no provision of automatic entry into archive, the operator will record the time, source, and type of alarm, and action taken. Results of investigations by the response force will be maintained at the monitor station. The historical record must be routinely reviewed by the responsible security officer. Records of alarm annunciations shall be retained for at least 90 days or until investigations of system violations and incidents have been successfully resolved and recorded.

UNCLASSIFIED

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

ANNEX C
(Effective 27 May 1994)

TACTICAL OPERATIONS/FIELD TRAINING

This annex pertains to specialized Sensitive Compartmented Information Facilities (SCIFs) deployed in a tactical operations or field training environment. It is divided into three parts to reflect the accepted modes of tactical operation:

Part I - Ground Operation

Part II - Aircraft/Airborne Operation

Part III - Shipborne Operation

C-1
UNCLASSIFIED

UNCLASSIFIED

DCID 1/21,

Annex C
Table of Contents

PART I GROUND OPERATION	
1.0 PURPOSE	5
2.0 APPLICABILITY AND SCOPE	5
3.0 RESPONSIBILITIES	6
4.0 ACCREDITATION OF TACTICAL SCIFs	6
5.0 PHYSICAL CONFIGURATION	7
6.0 TACTICAL SCIF OPERATIONS USING VANS, SHELTERS, AND VEHICLES	7
7.0 TACTICAL SCIF OPERATIONS WITHIN EXISTING PERMANENT STRUCTURES	7
8.0 MOBILE SIGINT SCIFs	7
9.0 SEMI-PERMANENT SCIFs	9
10.0 ELECTRICAL POWER	10
11.0 TEMPEST REQUIREMENTS	10
12.0 TELEPHONE EQUIPMENT	10
PART II AIRCRAFT/AIRBORNE OPERATION	
1.0 PURPOSE	11
2.0 APPLICABILITY	11
3.0 RESPONSIBILITIES	11
4.0 ACCREDITATION OF AIRCRAFT/AIRBORNE FACILITIES	11
5.0 POST AND PATROL REQUIREMENTS	12
6.0 ENTRY HATCHES	12
7.0 TEMPEST REQUIREMENTS	12
8.0 UNSCHEDULED AIRCRAFT LANDINGS	12
9.0 VOICE TRANSMISSIONS	13
10.0 DESTRUCTION REQUIREMENTS	13
PART III SHIPBOARD OPERATION	
1.0 PURPOSE	15
2.0 APPLICABILITY AND SCOPE	15
3.0 TYPES OF SHIPBOARD SCIFs (S/SCIFs)	15
4.0 PERMANENT ACCREDITATION	16
5.0 STANDARDS	16
6.0 INTRUSION DETECTION SYSTEM (IDS)	18
7.0 PASSING SCUTTLES AND WINDOWS	18
8.0 LOCATION OF CRYPTOGRAPHIC EQUIPMENT	18
9.0 SECURE STORAGE CONTAINERS	18
10.0 TELEPHONES	18
11.0 SECURE TELEPHONE UNIT-III (STU-III)	18
12.0 SOUND POWERED TELEPHONES	18
13.0 SCI INTERCOM ANNOUNCING SYSTEM	19
14.0 SUPPORTING INTERCOMMUNICATION ANNOUNCING SYSTEMS	19
15.0 COMMERCIAL INTERCOMMUNICATION EQUIPMENT	19
16.0 GENERAL ANNOUNCING SYSTEMS	19
17.0 PNEUMATIC TUBE SYSTEMS	20
18.0 DESTRUCTION EQUIPMENT	20

UNCLASSIFIED

19.0 EMERGENCY POWER	20
20.0 SCI PROCESSING SYSTEMS	20
21.0 TEMPORARY ACCREDITATION	20
22.0 TEMPORARY SECURE WORKING AREAS (TSWAs)	21
23.0 EMBARKED PORTABLE SHIPBOARD COLLECTION VANS (PSCVs)	22

PART I GROUND OPERATION:

1.0 PURPOSE:

This Annex prescribes the procedures for the physical security requirements for the operation of a Sensitive Compartmented Information Facility (SCIF) while in a field or tactical configuration, including training exercises. It also addresses the standards for truck mounted or towed trailer style shelters designed for use in a tactical environment but used in a garrison environment known as a Semi-permanent SCIF (SPSCIF).

2.0 APPLICABILITY AND SCOPE:

Recognizing that field/tactical operations, as opposed to operations within a fixed military installation, are of the type considered least secure, the following minimum physical security requirements will be met and maintained. Situation and time permitting, these standards will be improved upon using the security considerations and requirements for permanent secure facilities as an ultimate goal. If available, permanent-type facilities will be used. Under field or combat conditions, a continuous 24-hour operation is mandatory. Every effort must be made to obtain the necessary support from the host command (e.g., security containers, vehicles, generators, fencing, guards, weapons, etc.).

- 2.1 The Tactical SCIF (T-SCIF) shall be located within the supported headquarters defensive perimeter and preferably, also within the Tactical Operations Center (TOC) perimeter.
- 2.2 The T-SCIF shall be established and clearly marked using a physical barrier. Where practical, the physical barrier should be triple-strand concertina or General Purpose Barbed Tape Obstacle (GPBTO). The Tactical SCIF approval authority shall determine whether proposed security measures provide adequate protection based on local threat conditions.
- 2.3 The perimeter shall be guarded by walking or fixed guards to provide observation of the entire controlled area. Guards shall be armed with weapons and ammunition. The types of weapons will be prescribed by the supported commander. Exceptions to this requirement during peace may only be granted by the T-SCIF approval authority based on local threat conditions.
- 2.4 Access to the controlled area shall be restricted to a single gate/entrance, which will be guarded on a continuous basis.
- 2.5 An access list shall be maintained, and access restricted to those people whose names appear on the list.
- 2.6 The Tactical SCIF shall be staffed with sufficient personnel as determined by the on-site security authority based on the local threat conditions.
- 2.7 Emergency destruction and evacuation plans shall be kept current.
- 2.8 SCI material shall be stored in lockable containers when not in use.
- 2.9 Communications shall be established and maintained with backup response forces, if possible.

- 2.10 The SSO, or designee, shall conduct an inspection of the vacated Tactical SCIF area to ensure SCI materials are not inadvertently left behind when the T-SCIF moves.
- 2.11 Reconciliation of T-SCIF activation and operational data shall be made not more than 30 days after SCIF activation. Interim reporting of SCIF activities may be made to the CSA.

3.0 RESPONSIBILITIES:

The Cognizant Security Authority (CSA) is responsible for ensuring compliance with these standards and providing requisite SCI accreditation. The CSA may further delegate T-SCIF accreditation authority one command level lower. The Senior Intelligence Officer (SIO) is responsible when a temporary field or Tactical SCIF is used in support of field training exercises. During a period of declared hostilities or general war, a T-SCIF may be established at any level of accreditation upon the verbal order of a General or Flag Officer Commander.

4.0 ACCREDITATION OF TACTICAL SCIFs:

- 4.1 An Accreditation Checklist shall not be required for establishment of a T-SCIF. Approval authorities may require use of a local tactical deployment checklist.
- 4.2 The element requesting establishment of a T-SCIF shall notify the CSA, or designee, prior to commencement of SCIF operations. The message shall provide the following information:
 - 4.2.1 ID number of parent SCIF.
 - 4.2.2 Name of the Tactical SCIF.
 - 4.2.3 Deployed from (location).
 - 4.2.4 Deployed to (location).
 - 4.2.5 SCI level of operations.
 - 4.2.6 Operational period.
 - 4.2.7 Name of exercise or operation.
 - 4.2.8 Identification of facility used for T-SCIF operations (e.g., vans, buildings, tents).
 - 4.2.9 Points of contact (responsible officers).
 - 4.2.10 Description of security measures for entire operational period of SCIF.
 - 4.2.11 Comments.

5.0 PHYSICAL CONFIGURATION:

A T-SCIF may be configured using vehicles, trailers, shelters, bunkers, tents, or available structures to suit the mission. Selection of a T-SCIF site should first consider effective and secure mission accomplishment.

6.0 TACTICAL SCIF OPERATIONS USING VANS, SHELTERS, AND VEHICLES:

- 6.1 When a rigid side shelter or portable van is used for SCI operations, it shall be equipped with either a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA-approved lock. The combination to the lock or keys shall be controlled by the SSO at the security level for which the T-SCIF is accredited. The shelter or van shall be secured at all times when not activated as a SCIF.
- 6.2 The SCIF entrance of a radio frequency shielded enclosure designed for tactical operations may be secured with the manufacturer-supplied locking device or any combination of the locking devices mentioned above.

7.0 TACTICAL SCIF OPERATIONS WITHIN EXISTING PERMANENT STRUCTURES:

- 7.1 A T-SCIF may be operated within an existing structure when:
 - 7.1.1 Location is selected on a random basis.
 - 7.1.2 The location is not reused within a 36 month period. If reused within 36 months for SCI discussion, a TSCM evaluation is recommended.
- 7.2 There is no restriction over SCI discussion within a T-SCIF during war.

8.0 MOBILE SIGINT SCIFs:

- 8.1 A continuous 24-hour operation is mandatory.
- 8.2 The T-SCIF shall be staffed with sufficient personnel as determined by the on-site security authority based on the local threat conditions.
- 8.3 External physical security measures shall be incorporated into the perimeter defense plans for the immediate area in which the T-SCIF is located.
 - 8.3.1 A physical barrier is not required as a prerequisite to establish a mobile SIGINT T-SCIF.
 - 8.3.2 External physical security controls will normally be a function of the people controlling the day-to-day operations of the T-SCIF.
- 8.4 Communications shall be established and maintained with backup guard forces, if possible.
- 8.5 Emergency destruction plans shall incorporate incendiary methods to ensure total destruction of SCI material in emergency situations.

- 8.6 A rigid side shelter or a portable van are two possible configurations that may be used.
 - 8.6.1 When a rigid side shelter or portable van is used, it is subject to the following additional restrictions:
 - 8.6.1.1 If it is a shelter, it shall be mounted to a vehicle in such a way as to provide the shelter with the capability of moving on short notice.
 - 8.6.1.2 A GSA-approved security container shall be permanently affixed within the shelter. The combination to the lock will be protected to the level of security of the material stored therein.
 - 8.6.1.3 Entrance to the T-SCIF shall be controlled by SCI-indoctrinated people on duty within the shelter. When situations occur where there are no SCI-indoctrinated people within the shelter, i.e., during re-deployment, classified material shall be stored within the locked GSA container and the exterior entrance to the shelter will be secured.
 - 8.6.1.4 Entrance to the T-SCIF shall be limited to SCI-indoctrinated people with an established need-to-know whenever SCI material is used within the shelter.
 - 8.6.2 When a rigid side shelter or portable van is not available and a facility is required for SCI operations, such as in the case of a soft side vehicle or man-portable system, it is subject to the following additional restrictions:
 - 8.6.2.1 Protection will consist of an opaque container, i.e., leather pouch, metal storage box, or other suitable container that prevents unauthorized viewing of the material.
 - 8.6.2.2 This container shall be kept in the physical possession of an SCI-indoctrinated person.
- 8.7 The quantity of SCI material permitted within the T-SCIF will be limited to that which is absolutely essential to sustain the mission. Stringent security arrangements shall be employed to ensure that the quantity of SCI material is not allowed to accumulate more than is absolutely necessary.
 - 8.7.1 All working papers generated within the T-SCIF shall be destroyed at the earliest possible time after they have served their mission purpose to preclude accumulation of unnecessary classified material.
 - 8.7.2 If AIS equipment is used to store or process SCI data, a rapid and certain means of destruction shall be available to AIS operators to ensure the total destruction of classified material under emergency or combat conditions.
- 8.8 Upon cessation of hostilities, all classified material shall be returned to the parent element of the SCIF for reconciliation of records and destruction of obsolete material.

9.0 SEMI-PERMANENT SCIFs:

- 9.1 Vehicles with mounted shelters or towed trailer type shelters, designed for field or tactical use, that are employed as tactical SCIFs when deployed may also be used as a SCIF in nontactical situations if the SIO determines there is a need for more SCIF area and time and/or funds are not available to construct or enlarge a permanent SCIF. These types of SCIFs are SEMI-PERMANENT SCIFs (SPSCIFs).
- 9.2 The SPSCIF shall be accredited and operated in the same manner as a permanent SCIF. Requirements for TEMPEST and AIS accreditation apply as well.
- 9.3 The SPSCIF must be of rigid construction similar to a van, trailer, or transportable shelter. The construction material must be of such composition to show visible evidence of forced entry. Vents and air ducts must be constructed to prevent surreptitious entry. The doors must be solid construction and plumbed so the door forms a good acoustical seal. If installed, emergency exits and escape hatches must be constructed so they can only be opened from the interior of the SPSCIF.
- 9.4 The SPSCIF must be placed within a fenced compound on a military installation or equivalent, as determined by the CSA. The fence must be at least ten (10) feet from the SPSCIF and related building and equipment. The distance from the fence to the SPSCIF may have to be greater to provide acoustical security or to meet COMSEC or TEMPEST requirements. Access control to the fenced compound must be continuous.
- 9.5 All SPSCIFs must have a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA approved lock. (NOTE: Just as with combinations, keys require protection equivalent to the information which they protect.)
- 9.6 SPSCIFs do not need any additional security measures if one of the following exists:
- 9.6.1 Continuous operations. Continuous operations exist when the SPSCIF is occupied by one or more SCI-indoctrinated persons 24 hours a day. When there are multiple vehicles/shelters within a fenced compound, only those occupied by one or more SCI-indoctrinated people qualify as continuous operations facilities.
- 9.6.2 Dedicated guard force who have been subjected to a trustworthiness determination (e.g., NAC with no clearance to be issued). The dedicated guard force must be present whenever the SPSCIF is not occupied and must have continuous surveillance of the SPSCIF entrances. The guard force must check the perimeter of the SPSCIF at least twice an hour at random intervals. Guard response time will be five minutes or less.
- 9.7 SPSCIFs not storing classified material and not meeting one of the requirements in the above paragraphs may be required to have an Intrusion Detection System (IDS) as prescribed in ANNEX B as required by the CSA.
- 9.8 Requirements for storage when unoccupied:
- 9.8.1 SCI material will not be stored in a SPSCIF except when removal is not feasible, i.e., computer hard disk.

- 9.8.2 Storage in the United States and Outside the United States. If the SPSCIF does not have continuous operations or a dedicated guard force, a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA approved lock and an IDS for the SPSCIF interior is required. The interior SPSCIF IDS must be as prescribed in ANNEX B. The CSA may require exterior compound IDS.

10.0 ELECTRICAL POWER:

Electrical power supplied to T-SCIFs may be furnished by commercial or locally generated systems, as follows:

- 10.1 Tactical generator with access controls, including guards or surveillance of the generating equipment.
 - 10.1.1 The generating equipment shall be located within the protected perimeter of the organization supporting the T-SCIF. The generator shall not require location within the SCIF compound perimeter.
 - 10.1.2 Generator operator and maintenance people shall be US citizens.
- 10.2 In general, RF filters or isolators are not required for TEMPEST protection of commercial AC (alternating current) power lines used for SCI processing equipment in a T-SCIF.
- 10.3 Filtering and isolation generators (an electrical motor coupled to a generator by non-conductive means) may be used to provide isolated electrical power to the SCIF. The motor generator location shall be within the SCIF compound perimeter.

11.0 TEMPEST REQUIREMENTS:

Authority for TEMPEST accreditation of all compartments of SCI processed in a Tactical SCIF is delegated to the CSA based on review by the Certified TEMPEST Technical Authority (CTTA).

12.0 TELEPHONE EQUIPMENT:

Telephone instruments used within a T-SCIF shall meet requirements outlined in the Telephone Security ANNEX. Restrictions contained within the Telephone Security ANNEX pertaining to SCIF telephone services do not apply to T-SCIF operations during war.

PART II AIRCRAFT/AIRBORNE OPERATION:

1.0 PURPOSE:

This annex prescribes the physical security procedures for the operation of a Sensitive Compartmented Information Facility (SCIF) for aircraft, including airborne missions.

2.0 APPLICABILITY:

This annex is applicable to all aircraft to be utilized as a SCIF. Existing or previously accredited facilities do not require modification to conform with these standards.

3.0 RESPONSIBILITIES:

The CSA is responsible for ensuring compliance with these standards and providing SCI accreditation. The CSA may delegate aircraft/airborne SCIF accreditation authority to the major command level.

The major command/organization Senior Intelligence Officer (SIO) is responsible when an aircraft is used as a temporary SCIF in support of field training exercises. During a period of declared hostilities or general war, an aircraft/airborne SCIF may be established at any level of accreditation upon the verbal order of a General or Flag Officer Commander. The major command/organization is responsible for ensuring compliance with this annex.

4.0 ACCREDITATION OF AIRCRAFT/AIRBORNE FACILITIES:

- 4.1 An accreditation checklist will not be required for the establishment of an aircraft/airborne SCIF. Approval authorities may require use of a local deployment checklist, if necessary.
- 4.2 The element requesting establishment of an aircraft/airborne SCIF will notify the CSA prior to commencement of SCIF operations. The letter or message will indicate the following information:
 - Name of aircraft/airborne SCIF
 - Major command/organization
 - ID number of parent SCIF, if applicable
 - Deployed from (location) and dates
 - Deployed to (location) and dates
 - SCI level of operations
 - Name of exercise or operation
 - Points of Contact
 - Type of Aircraft and area to be accredited as a SCIF
 - Description of security measures for entire operational period of SCIF (SOP)
- 4.3 The SCIF will be staffed with sufficient personnel as determined by the on-site security authority based on the local threat environment.
- 4.4 SCI material will be removed from the aircraft on mission completion or at any landings, if feasible. When removal is not possible, or when suitable storage space/locations are not available, two armed (with ammunition) SCI-indoctrinated personnel must remain with the aircraft to control entry to the SCIF. Waivers to the requirement for weapons and ammunition may be approved on a case-by-case basis by the Commander.

- 4.5 The SSO or senior SCI-cleared person will conduct an inspection of the vacated SCIF to ensure SCI materials are not left behind.
- 4.6 Aircraft that transport SCI material incidental to travel between airfields do not require accreditation. However, compliance with directives pertaining to security of SCI material and communications is mandatory.

5.0 POST AND PATROL REQUIREMENTS:

Accredited aircraft require perimeter access controls, a guard force, and a reserve security team.

- 5.1 Unless protected by an approved IDS, hourly inspections will be made of all hatches and seals (including seal numbers).
- 5.2 A guard force and response team must be provided, capable of responding within five minutes if open storage is authorized, or 15 minutes for closed storage.
- 5.3 When aircraft are parked outside an established controlled area, a temporary controlled area must be established.

6.0 ENTRY HATCHES:

- 6.1 The aircraft commander or crew members will provide guard force personnel who have been subjected to a trustworthiness determination (e.g., NAC with no clearance to be issued) prior to departing from the immediate area of the aircraft.
- 6.2 All hatches will be locked to prevent unauthorized access. Hatches that cannot be secured from the outside will be sealed using serially numbered seals.

7.0 TEMPEST REQUIREMENTS:

Authority for TEMPEST accreditation of all compartments of SCI processed in an aircraft/airborne SCIF is delegated to the CSA, based on review by the Cognizant Certified TEMPEST Technical Authority (CTTA).

8.0 UNSCHEDULED AIRCRAFT LANDINGS:

- 8.1 US Military Bases: The local SSO or base security officer will be notified of the estimated arrival time and security protection required.
- 8.2 Other Airfields:
 - 8.2.1 Within the United States, the local Federal Aviation Administration (FAA) Security Officer will be notified of the estimated arrival time and security protection required.
 - 8.2.2 On arrival, the senior SCI-indoctrinated person is responsible for controlling entry and maintaining surveillance over the aircraft until all SCI material is secured in an accredited SCIF or the aircraft departs.

UNCLASSIFIED

- 8.2.3 Any properly accredited US Government SCIF may be used for temporary storage of materials from the aircraft. If the facility is not accredited for the level of information to be stored, the material must be double wrapped with initialed seals and stored in a GSA-approved security container.

8.3 Unfriendly Territory:

If an aircraft landing in unfriendly territory is anticipated, all SCI material will be immediately destroyed, with the destruction process preferably taking place prior to landing.

- 8.3.1 When flights are planned over unfriendly territory, SCI to be carried on board will be selected by the intelligence mission personnel and consist of the absolute minimum required for mission accomplishment.

- 8.3.2 All personnel will rehearse emergency destruction before each mission. Such emergency preparation rehearsals will be made a matter of record.

9.0 VOICE TRANSMISSIONS:

SCI discussions will only be conducted via appropriately encrypted aircraft radio.

10.0 DESTRUCTION REQUIREMENTS:

- 10.1 An Emergency Action Plan (EAP) will be written that provides for the evacuation and/or destruction of classified material. Evacuation plans and destruction equipment must be approved by the CSA and tested by mission personnel.
- 10.2 Emergency destruction and evacuation plans will be kept current.

PART III SHIPBOARD OPERATION:

1.0 PURPOSE:

This annex specifies the requirements for construction and security protection of SCIFs located on ships. The SCI accreditation checklist for ships may be obtained from the Director, Office of Naval Intelligence, 4301 Suitland Road, Washington, D.C. 20395.

2.0 APPLICABILITY AND SCOPE:

- 2.1 This annex is applicable to all new construction surface combatant ships. The application of this annex to surface non-combatants or sub-surface vessels will be referred to the CSA.
- 2.2 There may be instances in which circumstances constitute a threat of such proportion that they can only be offset by stringent security arrangements over and above those prescribed in this annex. Conversely, there may be instances in which time, location, mission, and/or condition of use of materials would make full compliance with these standards unreasonable or impossible. Such situations will be referred to the CSA for resolution on a case-by-case basis.
- 2.3 Existing or previously approved facilities do not require modification to conform with these standards.

3.0 TYPES OF SHIPBOARD SCIFs (S/SCIFs):

- 3.1 Permanent S/SCIFs: An area aboard ship where SCI operations, processing, discussion, storage, or destruction takes place. The area will have a clearly defined physical perimeter barrier and continuous physical security safeguards. The area may contain one or more contiguous spaces requiring SCIF accreditation. This type S/SCIF is routinely used during deployment and import operations.
- 3.2 Temporary S/SCIFs: An area aboard ship where temporary SCI operations, processing, discussion, storage, or discussion takes place. The area will have a clearly defined physical perimeter barrier and continuous physical security safeguards. The area may contain one or more contiguous spaces requiring SCIF accreditation. It will be continuously manned with sufficient SCI-cleared and -indoctrinated personnel, as determined by the on-site security authority based on the local threat environment, when SCI is present within the area. Temporary shipboard SCI operations will be limited to:
 - 3.2.1 A single deployment that will not exceed 12 months.
 - 3.2.2 A single mission requiring SCI operations that cannot be defined in length of operational time.
 - 3.2.3 During the period immediately preceding relocation of the ship to a refitting facility where the Temporary S/SCIF is scheduled for renovation and compliance with this annex. There will be a schedule established for renovation of the S/SCIF with confirmatory reporting of such to the CSA.

- 3.2.4 Temporary Platforms: A mobile or portable SCIF may be temporarily placed aboard a ship. Such platforms will be accredited on a temporary basis for a single deployment mission. The platform will be manned 24 hours a day by sufficient SCI-cleared and -indoctrinated personnel as determined by the on-site security authority. At the completion of the mission, the accreditation period will end and the CSA notified that the platform is certified clear and free of all SCI materials.

4.0 PERMANENT ACCREDITATION:

Ships requesting permanent accreditation status will provide to the CSA a complete inspection report and the Shipboard Inspection Checklist, certifying compliance with this Annex.

5.0 STANDARDS:

The physical security criteria for permanent S/SCIFs is as follows:

- 5.1 Physical Perimeter: The physical perimeter of an SCI space will be fabricated of structural bulkheads (aluminum or steel) with a thickness not less than 0.125 inch. Elements of the physical perimeter will be fully braced and welded in place.
- 5.2 Continuous SCI Spaces: Where several SCI spaces are contiguous to each other in any or all dimensions, the entire complex may be enclosed by a single physical perimeter barrier conforming to this annex.
- 5.2.1 Access to the SCI complex will be controlled by a single access door conforming to this annex. Each compartment within the complex may have a separate access door from within the common physical perimeter barrier. Such interior access control doors do not need to conform with this annex.
- 5.2.2 Access procedures will be established to ensure against cross-traffic of personnel not holding appropriate SCI access.
- 5.3 Normal Access Door: The normal access door will be a shipboard metal joiner door with honeycomb-core and fitted as specified below:
- 5.3.1 Where the normal access door is in a bulkhead that is part of an airtight perimeter, the airtight integrity may be maintained by collocating the airtight door with the metal joiner door, or by adding a vestibule.
- 5.3.2 The metal joiner door will be equipped with a combination lock that meets all requirements of Federal Specification FF-L-2740 or other CSA approved lock.
- 5.3.3 In addition to the lock, the door will be equipped with an access control device.
- 5.3.4 The door will be constructed in a manner that will preclude unauthorized removal of hinge pins and anchor bolts, as well as to obstruct access to lock-in bolts between door and frame.

UNCLASSIFIED

- 5.4 Emergency Exit: The emergency exit will be fabricated of aluminum plate or steel in accordance with this annex. The exit will be mounted in a frame braced and welded in place in a manner commensurate with the structural characteristics of the bulkhead, deck, or overhead in which it is situated.
- 5.5 Restriction on Damage Control Fittings and Cables: Because of the security restrictions imposed in gaining access to these spaces, no essential damage control fittings or cables will be located within or pass through an SCI space. This requirement is not applicable to damage control fittings, such as smoke dampers, that may be operated by personnel within the space during normal manning.
- 5.6 Removable Hatches and Deck Plates: Hatches and deck plates less than 10 square feet that are secured by exposed nuts and bolts (external to the SCI space) will be secured with externally attached, high security padlocks (unless their weight makes removal unreasonable). The padlock keys will be stored in a security container located within a space under appropriate security control.
- 5.7 Vent and Duct Barriers: Vents, ducts, or other physical perimeter barrier openings with a cross-sectional dimension greater than 96 square inches will be protected at the perimeter with a fixed barrier or security grill.
- 5.7.1 The grill will be fabricated of steel or aluminum grating or bars with a thickness equal to the thickness of the physical perimeter barrier. If a grating is used, bridge center-to-center measurements will not exceed 1.5 inches by 4 inches. Bars will be mounted on 6 inch centers. The grating or bars will be welded into place.
- 5.7.2 This requirement is not applicable to through ducts that have no opening into the space.
- 5.8 Acoustical Isolation: The physical perimeter barrier of all SCI spaces will be sealed or insulated with nonhardening caulking material to prevent inadvertent disclosure of SCI discussions or briefings from within the space, taking into account the normal ambient noise level, to persons located in adjacent passageways and/or compartments.
- 5.8.1 In cases where the perimeter material installation does not sufficiently attenuate voices or sounds of activities originating SCI information, the ambient noise level will be raised by the use of sound countermeasure devices, controlled sound generating source, or additional perimeter material installation.
- 5.8.2 Air handling units and ducts will be equipped with silencers or sound countermeasure devices unless continuous duty blowers provide a practical, effective level of masking (blower noise) in each air path. The effective level of security may be determined by stationing personnel in adjacent spaces or passageways to determine if SCI can be overheard outside the space.
- 5.9 Visual Isolation: Door or other openings in the physical perimeter barrier through which the interior may be viewed will be screened or curtained.

6.0 INTRUSION DETECTION SYSTEM (IDS):

The S/SCIF access door and emergency exit will be protected by a visual and audible alarm system. The installation will consist of sensors connected at each door and alerting indicators located at the facility supervisor's position. The normal access door alarm may have a disconnect feature.

- 6.1 Emergency exits will be connected to the alarm system at all times and will not have a disconnect feature installed.
- 6.2 The IDS will be connected to a remote alarm monitor station, which may be collocated with other IDS, and located within a space which is continuously manned by personnel capable of responding to or directing a response to an alarm violation at the protected space when it is unmanned.
- 6.3 Primary power for the IDS will be connected to an emergency lighting panel within the space. SCI spaces that are under continuous manning will be staffed with sufficient personnel, as determined by the on-site security authority based on the local threat environment, who have the continuous capability of detecting forced or surreptitious entry, without the aid of an IDS.

7.0 PASSING SCUTTLES AND WINDOWS::

Passing scuttles and windows will not be installed between SCI spaces and any other space on the ship.

8.0 LOCATION OF CRYPTOGRAPHIC EQUIPMENT:

On-line and off-line cryptographic equipment and terminal equipment processing SCI will be located only within the S/SCIF.

9.0 SECURE STORAGE CONTAINERS:

SCI material will be stored only in GSA approved Class 5, 6, or 7 security containers. Containers will be welded in place, or otherwise secured to a foundation for safety.

10.0 TELEPHONES::

Telephone instruments used within a S/SCIF will meet the Telephone Security Annex standards.

11.0 SECURE TELEPHONE UNIT-III (STU-III):

The STU-III Type 1 terminals may be installed within a S/SCIF.

12.0 SOUND POWERED TELEPHONES:

Where possible, sound powered telephones will be eliminated from S/SCIFs. Sound powered telephones located within the S/SCIF connecting to locations outside the S/SCIF will comply with the following:

- 12.1 The telephone cable will not break out to jackboxes, switchboards, or telephone sets other than at the designated stations. The telephone cable will not be shared with any circuit other than call or signal systems associated with the S/SCIF circuit.

UNCLASSIFIED

12.2 The telephone cable will be equipped with a selector switch, located at the controlling station, which is capable of:

12.2.1 Disconnecting all stations;

12.2.2 Selecting any one station and disconnecting the remaining stations; and

12.2.3 Parallel connection to all stations.

12.3 Other S/SCIFs located aboard the same ship, which have sound powered telephones not equipped with the required selector switch, will have a positive disconnect device attached to the telephone circuit.

12.4 Sound powered telephones within a S/SCIF that are not used for passing SCI information will have a sign prominently affixed to them indicating that they are not to be used for passing SCI.

12.5 A call or signal system will be provided. Call signal station, type ID/D, when used for circuit EM will be modified to provide a disconnect in the line to prevent a loud-speaker from functioning as a microphone.

13.0 SCI INTERCOM ANNOUNCING SYSTEM:

An intercommunication type announcing system processing SI that connects to or passes through areas outside the S/SCIF must be approved by the CSA.

14.0 SUPPORTING INTERCOMMUNICATION ANNOUNCING SYSTEMS:

Intercommunication-type announcing systems installed within an S/SCIF that do not process SCI information will be designated or modified to provide the following physical or electrical security safeguards:

14.1 Operational mode of the unit installed within the S/SCIF will limit operation to push-to-talk mode only.

14.2 Receive elements will be equipped with a local amplifier as a buffer to prevent loud-speakers or earphones from functioning as microphones.

14.3 Except as specified, radio transmission capability for plain radio telephone (excluding secure voice) will not be connected. Cable conductors assigned to the transmission of plain language radio telephones will be connected to ground at each end of the cable.

14.4 Equipment modified will have an appropriate field change label affixed to the unit that indicates the restriction. Additionally, the front panel will have a sign warning the user that the system is not passing classified information.

15.0 COMMERCIAL INTERCOMMUNICATION EQUIPMENT:

Commercial intercommunication equipment will not be installed within a S/SCIF without prior CSA approval.

16.0 GENERAL ANNOUNCING SYSTEMS:

General announcing system loudspeakers will have an audio amplifier, and the output signal lines will be installed within the S/SCIF.

17.0 PNEUMATIC TUBE SYSTEMS:

Pneumatic tube systems will not be installed. Existing systems will be equipped with the following security features:

- 17.1 Locked cover at both ends.
- 17.2 Capability to maintain the pressure or vacuum and capability to lock in the secure position at the initiating end.
- 17.3 Direct voice communications link between both ends to confirm the transportation and receipt of passing cartridges.
- 17.4 Special, distinctive color for SCI material passing cartridges.
- 17.5 Pneumatic tubes will run through passageways and will be capable of being visually inspected along their entire length.

18.0 DESTRUCTION EQUIPMENT:

A CSA-approved means of destruction of SCI material will be provided for each S/SCIF. Non-combatant surface ships that transit hostile waters without combatant escort will have appropriate Anti-Compromise Emergency Destruction (ACED) equipment on board and such equipment will be prepared for use. The ACED will be dedicated to SCI destruction. SCI material will not be destroyed by jettisoning overboard under any circumstances.

19.0 EMERGENCY POWER:

A S/SCIF will have emergency power available that will operate destruction equipment, alarm systems, access control devices, and emergency lighting equipment for a minimum of six hours.

20.0 SCI PROCESSING SYSTEMS:

A S/SCIF that processes SCI electronically or electrically should be provided a TEMPEST evaluation prior to activation. All computer and network systems that process SCI must be accredited or certified for operation by the cognizant SCI AIS Accreditation Authority.

21.0 TEMPORARY ACCREDITATION:

Ships requiring temporary accreditation status will be processed for accreditation upon completion of a physical security inspection and certification of compliance with the following security requirements:

- 21.1 If the space is used to electrically process SCI information, the CSA will make a TEMPEST evaluation based on threat.

UNCLASSIFIED

- 21.2 The physical perimeter barrier will consist of standard structural, nonsupport, or metal joiner bulkheads welded or riveted into place and meet the acoustical isolation requirements of a S/SCIF.
- 21.3 Doors will be at least metal joiner doors equipped with door closures and capable of being secured from the inside. Dutch doors are not acceptable. If cryptographic equipment is installed or stored within the space and the space will be temporarily unmanned while cryptographic key material and/or SCI material are stored elsewhere, the door will be equipped with a tamper-proof hasp and combination padlock.
- 21.4 Doors and other openings in the perimeter that permit aural or visual penetration of the internal space will be screened, curtained, or blocked.
- 21.5 An effective, approved secure means of destruction of SCI material will be readily available in the space or nearby in general service spaces.
- 21.6 Cryptographic equipment used to process SCI information will be located in the SCI space or, if located in a secure processing center other than that accredited for SCI, will be electrically configured so as not to be compatible with the secure processing system of that secure processor.
- 21.7 All telephones (to include STU-III instruments and sound powered telephones) will be as specified for S/SCIFs.
- 21.8 Processing of SCI via AIS will be as specified for S/SCIFs.

22.0 TEMPORARY SECURE WORKING AREAS (TSWAs):

Ships requiring TSWA accreditation for "contingency" or "part-time" usage will be processed for accreditation upon completion of a physical security inspection and certification of compliance with the following security requirements:

- 22.1 The physical perimeter barrier requires no special construction, provided it can prevent visual and aural access during all periods of SCI operation.
- 22.2 Doors will be capable of being secured from the inside.
- 22.3 Provisions will be made for posting a temporary sign that reads "RESTRICTED AREA - KEEP OUT - AUTHORIZED PERSONNEL ONLY".
- 22.4 When SCI material is to be stored in the space, a secure storage container will be provided. Security storage containers will be welded in place, or otherwise secured to the foundation for safety and to prevent rapid removal.
- 22.5 The electrical security requirements for a shipboard TSWA will be specified by the CSA.

23.0 EMBARKED PORTABLE SHIPBOARD COLLECTION VANS (PSCVs):

PSCVs are vans that are temporarily placed aboard ship and not part of the permanent structure of the ship. Ships requiring accreditation of embarked PSCVs must be annually accredited by the CSA and may be activated upon certification to the CSA of compliance with the following security requirements:

- 23.1 The exterior surface of the van will be solid construction and capable of showing evidence of physical penetration (except for intended passages for antenna cables, power lines, etc.)
- 23.2 The access door will fit securely and be equipped with a substantial locking device to secure the door from the inside in order to prevent forcible entry without tools.
- 23.3 Adequate security measures will be established to preclude viewing of classified material by uncleared personnel.
- 23.4 Adequate provisions will be established to control the approach of uncleared personnel within the vicinity of the van. These measures will consist of instructions promulgated by the station (ashore and afloat) in which the van is embarked, prohibiting loitering in the immediate vicinity of the van, and will include periodic visual security checks by appropriately SCI-indoctrinated personnel.
- 23.5 Adequate destruction equipment will be available and effective procedures established to ensure rapid and complete destruction of classified material in emergency situations.
- 23.6 All SCI material will be stored within the van and continuously manned by sufficient SCI-indoctrinated personnel as determined by the on-site security authority based on the local threat environment, when activated for SCI support. If SCI material is to be stored outside the van, the space must be accredited by the CSA and be in compliance with the above S/SCIF criteria.
- 23.7 The electrical security requirements for a PSCV will be as specified by the CSA.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

ANNEX D
(Effective 30 January 1994)

PART I

ELECTRONIC EQUIPMENT IN SENSITIVE COMPARTMENTED FACILITIES (SCIFS)

1.0 INTRODUCTION

It is the policy of the Director of Central Intelligence and the Senior Officials of the Intelligence Community (SOICs) that personally owned electronic equipment that has been approved for introduction into a SCIF should not be routinely carried into or out of the SCIF due to the possibility of technical compromise. It is also their policy that electronic equipment that is introduced into a SCIF is subject to technical and/or physical inspection at any time.

2.0 GUIDANCE

The following guidance is provided concerning the control of electronic equipment. SOICs retain the authority to apply more stringent requirements as deemed appropriate.

2.1 DOMESTIC UNITED STATES

The following personally owned electronic equipment may be introduced into a SCIF:

2.1.1 Electronic calculators, electronic spell-checkers, wrist watches, and data diaries. NOTE: If equipped with data-ports, SOICs will ensure that procedures are established to prevent unauthorized connector to automated information systems that are processing classified information.

2.1.2 Receive only pagers and beepers.

2.1.3 Audio and video equipment with only a "playback" feature (no recording capability), or with the "record" feature disabled/removed.

2.1.4 Radios

2.1.5 PROHIBITED EXCEPT FOR OFFICIAL DUTY

The following items are prohibited unless approved by the SOIC for conduct of official duties:

2.1.5.1 Two-way transmitting equipment.

2.1.5.2 Recording equipment (audio, video, optical). Associated media will be controlled.

2.1.5.3 Test, measurement, and diagnostic equipment.

2.1.6 PROHIBITED IN SCIFs

The following items are prohibited in SCIFs:

2.1.6.1 Personally owned photographic, video, and audio recording equipment.

2.1.6.2 Personally owned computers and associated media.

2.2 OVERSEAS

The provisions in paragraphs 2.1.5 and 2.1.6 above apply in the overseas environment with the exception that all personally owned electronic equipment may be introduced in the SCIF ONLY with the prior approval of the SOIC and on-site security representative, based on local threat conditions.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE 1/21

ANNEX D

Part II

DISPOSAL OF LASER TONER CARTRIDGES

1.0 INTRODUCTION

The Director of Central Intelligence and the Senior Officials of the Intelligence Community (SOICs) hereby establish the policy and procedures for disposing of used laser toner cartridges and drums. The policy established herein is based on the fact that exploitation of used toner cartridges is considered to be unlikely at this time; therefore, the expense of destroying toner cartridges is not deemed to be justified. SOICs are responsible for implementation of this policy within their respective department/agency. When deemed necessary and appropriate, SOICs may establish additional security measures.

2.0 POLICY

2.1 WITHIN CONUS, ALASKA, AND HAWAII

Used toner cartridges may be treated, handled, stored, and disposed of as UNCLASSIFIED, if, at a minimum, at least five full pages of unclassified, randomly generated text are run through the machine before the cartridge is removed. These pages should not include any blank spaces or solid black areas.

2.2 OVERSEAS

In addition to the sanitization measure described in paragraph 1, the drum must be adequately scored with an abrasive substance, e.g., sandpaper, to further reduce the opportunity for image recovery by rendering the drum unusable.

3.0 DENIAL OF ACCESS

3.1 The most likely avenue of technical penetration of reproduction equipment is through uncleared personnel. If exploitation of equipment is of concern to a SOIC, it is recommended that maintenance be conducted by appropriately cleared individuals. If this is not feasible, maintenance workers should be US citizens or be escorted and closely monitored by knowledgeable personnel.

3.2 In keeping with Environmental Protection Agency policy, agencies/departments are encouraged to establish procedures for recycling properly sanitized toner cartridges.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

ANNEX E
(Effective 30 January 1994)

ACOUSTICAL CONTROL AND SOUND MASKING TECHNIQUES

1.0 Basic Design:

Acoustical protection measures and sound masking systems are designed to protect SCI against being inadvertently overheard by the casual passerby, not to protect against deliberate interception of audio. The ability of a SCIF structure to retain sound within the perimeter is rated using a descriptive value, the Sound Transmission Class (STC).

- 1.1 The STC Rating: STC is a single number rating used to determine the sound barrier performance of walls, ceilings, floors, windows, and doors.
- 1.2 Use of Sound Groups: The current edition of Architectural Graphics Standards (AGS) describes various types of sound control, isolation requirements and office planning. The AGS established Sound Groups 1 through 4, of which Groups 3 and 4 are considered adequate for specific acoustical security requirements for SCIF construction.
 - 1.2.1 Sound Group 1 - STC of 30 or better. Loud speech can be understood fairly well. Normal speech cannot be easily understood.
 - 1.2.2 Sound Group 2 - STC of 40 or better. Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly if at all.
 - 1.2.3 Sound Group 3 - STC of 45 or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.
 - 1.2.4 Sound Group 4 - STC of 50 or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume, can be heard only faintly or not at all.

2.0 Sound Reduction for SCIFs:

The amount of sound energy reduction may vary according to individual facility requirements. However, Sound Group ratings shall be used to describe the effectiveness of SCIF acoustical security measures afforded by various wall materials and other building components.

- 2.1 All SCIF perimeter walls shall meet Sound Group 3, unless additional protection is required for amplified sound.
- 2.2 If compartmentation is required within the SCIF, the dividing office walls must meet Sound Group 3.

3.0 Sound Masking and Stand-Off Distance:

- 3.1 When normal construction and baffling measures have been determined to be inadequate for meeting Sound Group 3 or 4, as appropriate, sound masking shall be employed. Protection against interception of SCI discussions may include use of sound masking devices, structural enhancements, or SCIF perimeter placement:
 - 3.1.1 Sound masking devices may include vibration and noise generating systems located on the perimeter of the SCIF.
 - 3.1.2 Structural enhancements may include the use of high density building materials (i.e. sound deadening materials) to increase the resistance of the perimeter to vibration at audio frequencies.
 - 3.1.3 SCIF perimeter placement may include construction design of a stand-off distance between the closest point a non-SCI indoctrinated person could be positioned and the point when SCI discussions become available for interception. Use of a perimeter fence or protective zone between the SCIF perimeter walls and the closest "listening place" is permitted as an alternative to other sound protection measures.
- 3.2 Masking of sound which emanates from an SCI discussion area is commonly done by a sound masking system. A sound masking system may utilize a noise generator, tape, disc or record player as a noise source and an amplifier and speakers or transducers for distribution.

4.0 Placement of Speakers and Transducers:

To be effective, the masking device must produce sound at a higher volume on the exterior of the SCIF than the voice conversations within the SCIF. Speakers/transducers should be placed close to or mounted on any paths which would allow audio to leave the area. These paths may include doors, windows, common perimeter walls, vents/ducts, and any other means by which voice can leave the area.

- 4.1 For common walls, the speakers/transducers should be placed so the sound optimizes acoustical protection.
- 4.2 For doors and windows, the speakers/transducers should be close to the aperture of the window or door and the sound projected in a direction facing away from conversations.
- 4.3 Once the speakers or transducers are optimally placed, the system volume must be set and fixed. The level for each speaker should be determined by listening to conversations occurring within the SCIF and the masking sound and adjusting the level until conversations are unintelligible from outside the SCIF.

5.0 Installation of Equipment:

- 5.1 The sound masking system and all wires and transducers shall be located within the perimeter of the SCIF.

UNCLASSIFIED

- 5.2 The sound masking system shall be subject to review during TSCM evaluations to ensure that the system does not create a technical security hazard.

6.0 Sound Sources:

The sound source must be obtained from a player unit located within the SCIF. Any device equipped with a capability to record ambient sound within the SCIF must have that capability disabled. Acceptable methods include:

- 6.1 Audio amplifier with a record turntable.
- 6.2 Audio amplifier with a cassette, reel-to-reel, Compact Disc (CD), or Digital Audio Tape (DAT) playback unit.
- 6.3 Integrated amplifier and playback unit incorporating any of the above music sources.

7.0 Emergency Notification Systems:

The introduction of electronic systems that have components outside the SCIF should be avoided. Speakers or other transducers, which are part of a system that is not wholly contained in the SCIF, are sometimes required to be in the SCIF by safety or fire regulations. In such instances, the system can be introduced if protected as follows:

- 7.1 All incoming wiring shall breach the SCIF perimeter at one point. TEMPEST or TSCM concerns may require electronic isolation.
- 7.2 In systems that require notification only, the system shall have a high gain buffer amplifier. In systems that require two-way communication, the system shall have electronic isolation. SCIF occupants should be alerted when the system is activated. All electronic isolation components shall be installed within the SCIF as near to the point of SCIF egress as possible.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

ANNEX F

(Effective 30 January 1994)

PERSONNEL ACCESS CONTROLS

1.0 Access Controls:

The SCIF perimeter entrance should be under visual control at all times during duty hours to preclude entry by unauthorized personnel. This may be accomplished by several methods (e.g., employee work station, guard, CCTV). Regardless of the method utilized, an access control system shall be used on the SCIF entrance. Persons not SCI-indoctrinated shall be continuously escorted within a SCIF by an SCI-indoctrinated person who is familiar with the security procedures of that SCIF.

1.1 Automated Access Control Systems¹: An automated access control system may be used to control admittance to SCIFs during working hours in lieu of visual control, if it meets the criteria stated below.

1.1.1 The automated access control system must identify an individual and authenticate that person's authority to enter the area through the use of an identification (ID) badge or card, or by personal identity verification. Automated identification of individuals exiting the area is desirable.

1.1.1.1 ID Badges or Cards. The ID badge or card must use embedded sensors, integrated circuits, magnetic stripes or other means of encoding data that identifies the facility and the individual to whom the card is issued.

1.1.1.2 Personal Identity Verification. Personal identity verification (Biometrics Device) identifies the individual requesting access by some unique personal characteristic, such as:

- (a) Fingerprinting,
- (b) Hand Geometry,
- (c) Handwriting,
- (d) Retina, or
- (e) Voice recognition.

1.1.2 In conjunction with 1.1.1.1 above, a personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual. The PIN must be changed when it is believed to have been compromised or subjected to compromise.

¹Manufacturers of automated access control equipment or devices must assure in writing that their system will meet the following standards before CSA's may favorably consider such systems:
Chances of an unauthorized individual gaining access through normal operation of the equipment are no more than one in ten thousand;
Chances of an authorized individual being rejected for access through normal operation of the equipment are no more than one in one thousand.

- 1.1.3 Authentication of the individual's authorization to enter the area must be accomplished within the system by the inputs from the ID badge/card or the personal identity verification device or the keypad with an electronic data base of individuals authorized into the area. A procedure must be established for removal of the individual's authorization to enter the area upon reassignment, transfer or termination, or when the individual's access is suspended, revoked, or downgraded to a level lower than required.
- 1.1.4 Physical security protection must be established and continuously maintained for all devices/equipment that constitute the system. The level of protection may vary depending upon the type of devices/equipment being protected with the basic intent of utilizing the security controls already in effect within the facility.
- 1.1.4.1 Locations where authorization data, card encoded data and personal identification or verification data is input, stored, or recorded must be protected within a SCIF or controlled by SCI indoctrinated personnel.
- 1.1.4.2 Card readers, keypads, communication or interface devices located outside the entrance to a controlled area shall have tamper resistant enclosures, and be securely fastened to a wall or other structure. Control panels located within a controlled area shall require only a minimal degree of physical security protection sufficient to preclude unauthorized access to the mechanism.
- 1.1.4.3 Keypad devices shall be designed or installed in such a manner that an unauthorized person in the immediate vicinity cannot observe the selection of input numbers.
- 1.1.4.4 Systems that utilize transmission lines to carry access authorizations, personal identification, or verification data between devices/equipment located outside the controlled area shall receive a minimum of Class II line supervision, as described in Annex B.
- 1.1.4.5 Electric strikes used in access control systems shall be heavy duty industrial grade.
- 1.1.5 Access to records and information concerning encoded ID data and PINs shall be restricted to individuals appropriately indoctrinated at the same level as the information contained within. Access to identification or authorization data, operating system software or any identifying data associated with the access control system shall be limited to the fewest number personnel as possible. Such data or software shall be kept secure when unattended.
- 1.1.6 Records shall be maintained reflecting active assignment of ID badge/card, PIN, level of access, access, and similar system-related records. Records concerning personnel removed from the system shall be retained for 90 days. Records of entries to SCIFs shall be retained for at least 90 days or until investigations of system violations and incidents have been successfully resolved and recorded.

UNCLASSIFIED

- 1.1.7 Personnel entering or leaving an area shall be required to immediately secure the entrance or exit point. Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's access and need-to-know.
- 1.2 Electric, Mechanical, or Electromechanical Access Control Devices. Electric, mechanical, or electromechanical devices which meet the criteria stated below may be used to control admittance to SCIF areas during working hours if the entrance is under visual control. These devices are also acceptable to control access to compartmented areas within the SCIF. Access control devices must be installed in the following manner:
 - 1.2.1 The electronic control panel containing the mechanical mechanism by which the combination is set will be located inside the SCIF. The control panel (located within the SCIF) will require only a minimal degree of physical security designed to preclude unauthorized access to the mechanism.
 - 1.2.2 The control panel shall be installed in such a manner, or have a shielding device mounted, so that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination.
 - 1.2.3 The selection and setting of the combination shall be accomplished by an individual cleared at the same level as the highest classified information continued within. The combination shall be changed as required in Chapter 2.6.
 - 1.2.4 Electrical components, wiring included, or mechanical links (cables, rods and so on) should be accessible only from inside the SCIF, or if they traverse an uncontrolled area they shall be secured within a protective covering to preclude surreptitious manipulation of components.

DIRECTOR OF CENTRAL INTELLIGENCE DIRECTIVE (DCID) 1/21

ANNEX G
(Effective 29 July 1994)

TELEPHONE SYSTEMS and EQUIPMENT

1.0 PURPOSE

This Annex specifies the requirements and procedures for systematically incorporating Telephone Security Group (TSG) approved telephone security measures into the planning, installation, maintenance, and management of telephone service for SCIFs within and outside the United States.

2.0 DEFINITIONS

- 2.1 **ADMINISTRATIVE TELEPHONE.** A telephone intended for unclassified conversation. This designation specifically excludes secure-voice systems unless they incorporate a non-secure mode of operation.
- 2.2 **DISCONNECT DEVICE.** A device that [1] inserts a break at some point in the normal hardwire conduction path that exists between a telephone and its telecommunications medium, and [2] only when the telephone is in the in-use (off-hook) state, establishes a temporary metallic connection across that break.
- 2.3 **ISOLATOR.** A device that [1] inserts a break at some point in the normal hardwire conduction path that exists between a telephone and its telecommunications medium, and [2] only when the telephone is in the in-use (off-hook) state, provides a temporary communication channel across that break without establishing an end to end metallic connection.
- 2.4 **OFF-HOOK.** A terminal is off-hook when its signaling protocol to its network controller specifies that there is an intention to initiate, accept, or maintain communications with some other terminal.
- 2.5 **ON-HOOK.** This condition refers to a network communications line and simultaneously to all the terminals connected to that line. A terminal is on-hook when it is not off-hook; its signaling protocol to its network controller specifies that there is no intention to initiate, accept, or maintain communications with any other line or terminal. For a telephone to be considered on-hook, the handset must be in the handset cradle and all speakerphone and hands-free functions must be turned off.
- 2.6 **TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM).** Techniques and measures used to detect and nullify hostile penetration technologies, which are used to obtain unauthorized access to sensitive information. TSCM also includes the development and use of protective systems to detect and/or deter hostile penetration attempts and the hostile exploitation of naturally occurring hazards.
- 2.7 **TELEPHONE SYSTEM.** The telephone installation that provides service to the SCIF, and includes but is not limited to: all equipment, hardware, wiring, features, software, and supporting systems.

- 2.8 TSG. The TSG (Telephone Security Group) is the primary technical and policy resource in the National Advisory Group/Security Countermeasures (NAG/SCM) structure for all aspects of the TSCM program that involve telephones or telephone systems.
- 2.9 TYPE-ACCEPTED TELEPHONES. These are specially configured telephone models that are warranted by their manufacturers to incorporate specific TSG-mandated security measures. On-hook telephone security protection is an intrinsic property for TYPE-ACCEPTED TELEPHONES and they may be installed without ancillary isolation or disconnect devices. (See Standard 6.)
- 2.10 UNATTENDED OFF-HOOK AUDIO SECURITY. Security measures intended to prevent the compromise of background conversations when the user temporarily leaves the instrument off-hook. (See Standard 1.)

3.0 APPLICABILITY AND SCOPE

- 3.1 Administrative telephone system installations must include security measures that balance the vulnerabilities of the system against the technical threats of its environment.
- 3.2 This Annex is compatible with but may not satisfy requirements of other security disciplines such as COMSEC, OPSEC, or TEMPEST.
- 3.3 The telephone security measures of this Annex apply to any telephone system that provides service to a SCIF.
- 3.4 This Annex does not apply if the SCIF is declared a "No Classified Discussion Area" and warning notices are posted prominently within the SCIF.

4.0 REFERENCES

The below-listed TSG standards are available to all members of the United States Intelligence Community from their respective cognizant security authorities (CSAs). Individual standards may be released to non-government personnel following CSA determination of the need. Any such release is to be accompanied by a letter identifying the standard as an official US Government document that may not be disseminated further without specific approval of the issuing agency.

- 4.1 Standard 1, Introduction to Telephone Security. Provides telephone security background and TSG-approved options for telephone installations in US Government sensitive discussion areas. For use by all personnel concerned with telephone security.
- 4.2 Standard 2, TSG Guidelines for Computerized Telephone Systems. Establishes requirements for planning, installing, maintaining, and managing a CTS. For personnel involved in writing contracts, planning, installing, maintaining, inspecting, and system administration.
- 4.3 Standard 3, Type-Accepted Program for Telephones Used With the Conventional Central Office Interface. Identifies a program that outlines specifications for design and manufacture and procedures required for type-acceptance. For personnel involved in writing contracts, manufacturing, and inspecting.

- 4.4 Standard 4, Type-Acceptance Program for Electronic Telephones Used in Computerized Telephone Systems. Identifies a program that outlines specifications for design and manufacture and procedures required for type-acceptance. For personnel involved in writing contracts, manufacturing, and inspecting.
- 4.5 Standard 5, On-Hook Telephone Audio Security Performance Specifications. Specifies the amount of audio leakage allowed in the on-hook condition of telephones without disconnects. For personnel involved in writing contracts, manufacturing, and inspecting telephones such as STU-III's.
- 4.6 Standard 6, Telephone Security Group-Approved Equipment. Lists TSG-approved equipment. For all personnel concerned with procurement and use of TSG-approved equipment.
- 4.7 Standard 7, TSG Guidelines for Cellular Telephones. Provides guidelines for the manufacture and use of secure and non-secure cellular telephones in US Government sensitive discussion areas. For personnel involved in writing contracts, manufacturing, inspecting, maintaining, and using cellular telephones.
- 4.8 Standard 8, Microphonic Response Criteria for Non-Communications Devices. Specifies the maximum audio response allowed for isolation devices and other non-communication equipment used in US Government sensitive discussion areas. For personnel involved in writing contracts, manufacturing, installing, and inspecting telephone-related equipment.
- 4.9 Standard 9, TSG Approval Program for Secure Telephones and Equipment That Connect to the Conventional Central Office Interface. Specifies TSG requirements for secure telephones and equipment interfacing with the conventional central office. For personnel involved in writing contracts, manufacturing, and inspecting TSG approved telephones.

5.0 RESPONSIBILITIES

- 5.1 TSG: The TSG is responsible for evaluating vulnerabilities of telephone systems and identifying security countermeasures.
- 5.2 CSA: The CSA is responsible for selecting, implementing, and verifying security measures to balance the vulnerabilities of the telephone system against the technical threats of its environment. This requires the CSA to:
 - 5.2.1 Assist Special Security Officers (SSOs) and Contractor Special Security Officers (CSSOs) in selecting the most cost effective countermeasures.
 - 5.2.2 Maintain a current set of TSG standards.
 - 5.2.3 Provide written waivers to any requirements of this Annex and TSG standards. In granting waivers, the CSA accepts full responsibility for the associated risks.

- 5.2.4 Request technical surveillance countermeasures (TSCM) inspections as conditions warrant to prevent the loss or compromise of intelligence sources and methods, including sensitive compartmented information, through adversary use of technical surveillance.
- 5.3 SSO/CSSO: The SSO/CSSO is responsible for requesting CSA approval for new telephone systems and major modifications to existing systems by:
 - 5.3.1 Submitting necessary documentation on new systems and any changes to existing systems to the CSA for evaluation.
 - 5.3.2 Maintaining the documentation on-site.

6.0 REQUIREMENTS

- 6.1 ACCESS CONTROL: Installation and maintenance personnel will possess the appropriate security clearance as determined by the CSA. Uncleared installation and maintenance personnel given access to the SCIF should be US citizens and will be monitored by escorts.
- 6.2 CABLE CONTROL:
 - 6.2.1 All telephone wire and fiber optic (fiber) conductor cables should enter the SCIF through a common opening.
 - 6.2.2 Each conductor should be accurately accounted for from the point of entry. The accountability should identify the precise use of every conductor through labeling, log, or journal entries.
 - 6.2.3 Unused conductors will be removed. If removal is not feasible, the CSA may require that metallic conductors be stripped, bound together, and grounded.
 - 6.2.4 Unused fiber conductors will be uncoupled from the interface within the SCIF.
- 6.3 ON-HOOK SECURITY:

Approved points of on-hook isolation may be provided by any of the following:

 - 6.3.1 The telephone, disconnect, or isolator, if TSG approved. Standard 6, available from the CSA, lists TSG-approved equipment and ordering information.
 - 6.3.2 The telephone switch, if it meets the requirements of Standard 2.
 - 6.3.3 With CSA approval, isolation may be provided by the telephone switch not meeting TSG Standard 2 provided that:
 - 6.3.3.1 Access to the facility housing the telephone switch is controlled.

6.3.3.2 All communication lines between the telephone switch and the SCIF are in controlled space and inspectable by government or contractor security personnel and technically qualified telephone personnel.

6.3.3.3 No SCIF telephone or other device with a speaker can be forced "off-hook" via a software command from the telephone switch or forced to remain "off-hook" after a user has terminated the conversation.

6.4 OFF-HOOK SECURITY:

Unattended off-hook security may be accomplished by one of the following:

6.4.1 Use of a hold or mute feature that does not allow audio from the telephone to leave the controlled area.

6.4.2 A push-to-operate handset will be required if an appropriate hold feature is not available. (See Standard 6.)

6.5 RESTRICTIONS.

6.5.1 Personally owned equipment that can interface with the telephone system is prohibited.

6.5.2 Speakerphones are designed to pick up and transmit nearby conversation when they are in use. Therefore, speakerphones are restricted from common-use office areas where sensitive conversations might be unknowingly intercepted. Prior CSA approval is required for speakerphones in sole-use offices.

6.5.3 Telephone Answering Devices (TADs) may have features which are security vulnerabilities, e.g., remote room monitoring. Prior CSA approval is required for TADs.

**Lessons Learned about
Construction or Alteration of
Department of Defense (DOD)
Sensitive Compartmented Information Facilities (SCIF)**

1. Purpose. The purpose of this paper is to inform persons involved in the construction or alteration of DOD SCIF's of changes in criteria. The intelligence community coordinated and adopted one criteria document, Director of Central Intelligence Directive (DCID) 1/21 "Physical Security Standards for Sensitive Compartmented Information Facilities" dated 30 January 1994.
2. Limits of this Paper. This paper is to supplement, not repeat, DCID 1/21 with "lessons learned" at the Director of Central Intelligence (DCI) training course on DCID 1/21. It is not meant to be all encompassing.
3. Asset and SCIF Use. A SCIF is an area in which sensitive compartmented information (SCI) is stored, processed, or spoken. The stored SCI may be in the form of paper, removable magnetic media, and "embedded" non-removable media.
4. Criteria Documents. SCIF's were previously constructed in accordance with Defense Intelligence Agency Manual (DIAM) 50-3, which has been replaced by DCID 1/21. The DCID 1/21 has less restrictive physical security standards, which will result in a significant savings on construction. Special Access Programs (SAP's) did not adopt DCID 1/21.
5. Operations. Co-utilization of SCIF and SAP areas is recommended to require less SCIF construction and compartmenting. DCID 1/21 no longer requires the two persons for staffing. COMSEC requirements must be considered.
6. SCIF Accreditation. The intelligence community has staffed a combined agency accreditation and inspection office. Coordinate new or renovated SCIF's with the accreditation office. The accreditation office checks for compliance with DCID 1/21 and reviews the TEMPEST accreditation as well. This must be done on a case-by-case basis. For DOD SCIF's, the accreditation office for required construction and TEMPEST countermeasures is Defense Intelligence Agency (DIA), Accreditation Management Branch (DAC-2A). DIA points of contact may be reached by phone at (703) 907-1299 for assistance.
 - a. SCIF Accreditation Submissions. At a minimum of 30 percent design completion, the security officer must send drawings and a description of the facility to DIA. Mail this submission directly to DIA and an information copy to the MACOM. DIA will review the submission in 10 working days and report to the sender. DIA prefers the security officer send floor plans which indicate the SCIF perimeters, the access control system, and the alarm and intrusion detection system (IDS) layout. The security officer also should indicate security related features such as SCIF wall, floor, and ceiling construction (including sound

transmission class (STC) rating); SCIF doors and windows; and penetrations through SCIF walls, floors, and ceilings (including grills or bars). Please do not send the entire construction package.

b. TEMPEST Accreditation. TEMPEST accreditation will be considered during the design process. There are two relatively new documents that govern TEMPEST design. They are NSTISS No. 300, "National Policy on Control of Compromising Emanations" (FOUO) dated 29 November 1993, and NSTISS No. 7000, "TEMPEST Countermeasures for Facilities" (C) dated 29 November 1993. Before incorporating any countermeasures, contact the accreditation office. The DCID 1/21 contains requirements on "Red/Black" power separation and on telephones and wiring.

7. Physical Security and Safety Standards. SCIF's are designed to provide security for stored and/or processed SCI. SCIF's must also provide for the safety of the persons inside, as in the case of an emergency evacuation due to a fire. SCIF design must comply with NFPA 101 Life Safety Code, your applicable building code, and the Americans with Disabilities Act. Refer to Appendix A for a concise overview of NFPA and BOCA requirements. The security features of a SCIF may not be at the expense of safety features. When designing a SCIF, schedule a joint security/safety meeting and discuss items such as locking and exiting. Explain the intent of the security features to the fire marshall. And whatever you do, do not upset the fire marshall. In a disagreement over security features versus safety features, safety features will govern because past litigation has been against security. Design to satisfy both, rather than seeing it as security versus safety.

8. IDS and Access Control. DCID 1/21 requires SCIF's to have IDS and access control. The IDS is either on the asset itself or around the perimeter, but not both. Also, IDS is no longer required below raised floors and above false ceilings that are within the SCIF perimeter boundary. Fewer sensors are required by DCID 1/21 than were by the DIAM 50-3. For the IDS to be effective, an unauthorized entry into a SCIF must send an alarm to a response force. The time in which the force must respond depends upon how the SCI is stored, and the construction standards. Refer to figure 1.

9. Construction. Construction is dictated by the SCIF location and how the SCI is stored.

a. Walls. The walls will be either drywall, expanded metal, or vault construction as required (refer to figure 1). SCIF's located on a military compound in the continental U.S. typically will use the DCID 1/21 "drywall" construction standards. Additionally, if SCI is spoken at normal conversation levels (not amplified), the wall should be designed to an STC of 45. The instructors in class emphasized that the walls must go from true floor slab to true roof construction, or floor slab of next story, (not just to underside of a suspended ceiling). This said, there are cases when one should not construct true floor to true roof walls, because the space above the ceiling is used as the mechanical system's return air plenum or because existing utilities above the ceiling prohibit construction, such as mechanical ducts, utility lines, electrical power busses, and water lines. In these cases, the designer must

design the ceiling to be equivalent to the required walls, with careful attention to sound transmission.

b. **STC Rated Walls.** The STC rated wall design, recommended in the class, is depicted in figure 2. This is an excellent wall design because sound is not transferred through the drywall to the stud and out because the acoustical insulation is continuous and is not crushed around the electrical outlets and power boxes. With minor design modification, this wall can achieve the range of STC ratings required by the DCID 1/21.

c. **Floor, Roof/Ceiling.** The floor and roof construction depends on the drywall, expanded metal, or vault construction required. Typically floors on grade and floor slabs between stories exceed the drywall and expanded metal requirements.

d. **Doors.** Construction guidance for doors in the DCIC 1/21 is quite specific.

(1) **Entry Vestibule.** A vestibule arrangement for SCIF entry doors is recommended when the requirements of locking, exiting, and an STC rating are required on one door. Provide a lock on the outer door for access control to the vestibule (such as the Unicam 1000) and use the required combination lock on the interior door. Coordinate locking arrangement with the accreditation office. If the SCIF is required to have an STC rating of 45, the vestibule arrangement with non-rated doors is usually acceptable. This is because some discernable speech may enter the vestibule but only personnel with access will be in this vestibule. Speech is typically not discernable outside of the vestibule.

(2) **Second Door.** It is possible due to the locking arrangement on the SCIF entry door that it will not be regarded as an approved exit. If an exit is required, provide a second door next to the entry door with exit only hardware.

(3) **STC Rated Doors.** Do not use an electric strike with an STC rated door. The pressure caused by the acoustical gasketing binds the electric strike.

e. **Door Locks.** Suggested locks for various door locations in SCIF's are shown in figure 3.

f. **Windows.** For SCIF's located on a military compound in the continental U.S., windows typically will not be required to be forced entry resistant. Windows able to provide forced entry resistance equivalent to expanded metal standards are costly but are available. Specify they provide 5 or 15 minutes of delay to forced entry resistance when tested using State Department standard SD-STD-01.01 Revision G (Amended) "Certification Standard Forced Entry and Ballistic Resistance of Structural Systems." Alternatively, windows can be designed with very heavy mullions and a maximum lite size of 96 square inches. Windows may also be required to be STC rated to preclude inadvertent disclosure of spoken SCI. Windows also need to be obscured when SCI is visible (which negates some of the purpose

of the windows). Blinds or curtains are acceptable for obscuration. Alternatively, figured, distorted, or translucent glazing or glass block should be acceptable.

h. Openings Above 96 Square Inches. Mechanical openings and penetrations into SCIF's above 96 square inches shall have bars, grills, or commercial metal duct sound baffles as discussed in DCID 1/21. DCID 1/21 alternatively allows IDS to be placed in the opening.

10. Spoken Information. If there is a possibility of inadvertent disclosure of spoken SCI, the perimeter of the SCIF may be required to be sound rated. DCID 1/21 also allows the use of sound masking systems. Using ASTM E 90, STC ratings are determined under laboratory conditions on construction samples with no defects (a blank wall panel). In reality, construction has many paths for sound to go through: electrical boxes, conduit, mechanical penetrations, joints between different materials, and planar intersections of materials (such as roof to wall.) To compensate, the designer needs to choose elements slightly beyond the desired STC rating and detail all penetrations and intersections to show proper construction and sealant. Proper detailing should ensure there is no need to perform field tests using ASTM E 336 to determine the noise reduction coefficients of the space. This test is expensive, time consuming, requires the SCIF space to be completely enclosed, and requires absolute quiet outside the space.

11. Collateral Storage. If a space has been designed and accredited for open storage of SCI, collateral storage needs no further protection.

12. Plans and Specifications. On the drawings and in the specifications, do not use: the word SCIF, program names, or names of individuals. Use generic names like office space, laboratory space, shop, etc. Other information should be provided in the analysis of design that does not go to contractor. The security officer uses the design analysis and drawings to make the accreditation submission.

13. The point of contact on this paper is Mary Nelson Darling, Army Corps of Engineers Protective Design Mandatory Center of Expertise. Please call me at (402) 221-4924 if you have any questions.

COMMON LIFE SAFETY REQUIREMENTS

Working Definitions¹:

Means of Egress: A means of egress is a continuous and unobstructed way of exit travel from any point in a building or structure to a public way and consists of three separate and distinct parts: (a) the exit access, (b) the exit, and (c) the exit discharge. A means of egress comprises the vertical and horizontal travel and shall include intervening room spaces, doorways, hallways, corridors, passageways, balconies, ramps, stairs, enclosures, lobbies, escalators, horizontal exits, courts, and yards.

Exit: Exit is that portion of a means of egress that is separated from all other spaces of the building or structure by construction or equipment as required to provide a protected way of travel to the exit discharge. Exits include exterior exit doors, exit passageways, horizontal exits, and separated exit stairs or ramps.

Exit Access: Exit access is that portion of a means of egress that leads to an exit.

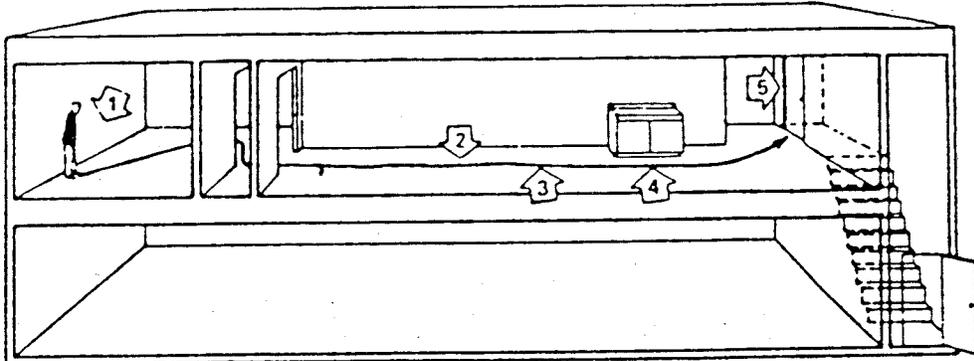
Exit Discharge: Exit discharge is that portion of a means of egress between the termination of an exit and a public way.

Common Path of Travel: Common path of travel is that portion of exit access that must be traversed before two separate and distinct paths of travel to two exits are available. Paths that merge are common paths of travel. Common path of travel is measure in the same manner as travel distances but terminates at that point where two separate and distinct routes become available.

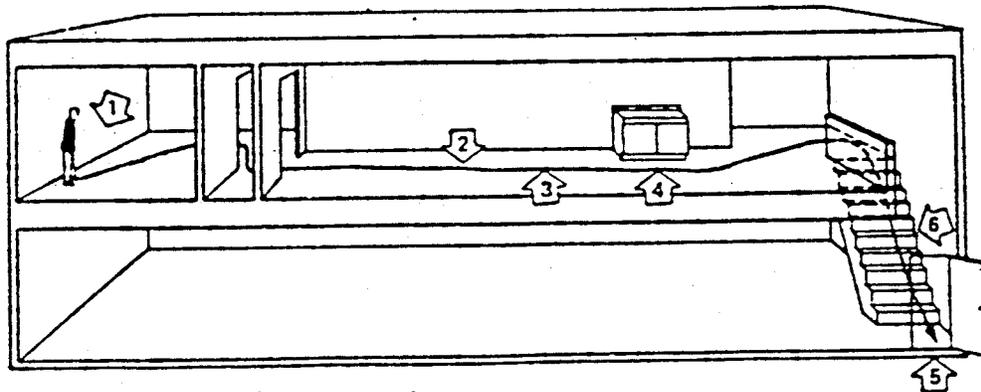
Dead End Corridor: A dead end corridor occurs where an occupant may enter a corridor or space thinking there is an exit at the end and, finding none, must retrace his or her path to again reach a choice of exits.

¹ Definitions taken from the 1991 Life Safety Code Handbook

Figures 5-60a and b. Measuring Travel Distance to an Exit. In Figure 5-60a the stair is enclosed to meet the requirements of an exit enclosure, whereas in Figure 5-53b the stair is not enclosed.



- Travel distance is measured:
- 1 - starting 1 foot from the most remote point,
- 2 - along the center line of the natural path of travel,
- 3 - on the floor or other walking surface,
- 4 - curving around corners/obstructions with a clearance of 1 foot,
- 5 - ending where exit begins



- Travel distance is measured:
- 1 - starting 1 foot from the most remote point,
- 2 - along the center line of the natural path of travel,
- 3 - on the floor or other walking surface,
- 4 - curving around corners/obstructions with a clearance of 1 foot,
- 5 - ending where exit begins
- 6 - travel distance includes travel over open stairs and ramps; stairs are measured in the plane of the tread nosing

Six-Unit Condominium

Two Die When Security Bars Prevent Escape; California

A 40-YEAR-OLD WOMAN AND HER 17-YEAR-OLD SON died in their new home when a lighted candle apparently fell off the dining room table into some paper and cardboard boxes piled on the floor. The two had recently moved into the two-story wood-frame condominium, which was built in 1970. The 700-square-foot structure was not equipped with smoke detectors.

The fire was reported by another occupant of the condominium, who called the fire department at 12:51 am. When firefighters arrived, they found smoke and flames issuing from the unit and called for a second alarm as crews began trying to rescue the two trapped victims and extinguish the blaze.

Firefighters found the woman's body inside the first-floor doorway, and her son's in an upstairs bedroom. Security bars on all the windows and doors had prevented them from escaping. They also prevented the family's neighbors from rescuing them. One man was able to kick in the solid wood front door through the closed security gate, only to see the woman beyond reach, her clothing in flames.

Trapped by Security Bars, Three Die in Apartment Blaze

California

A 40-year-old father and his two sons, ages 8 and 4, died when fire broke out in their apartment and all escape routes were compromised by a multitude of security features.

The two-story, eight-unit, wood-and-stucco apartment building measured 120 feet by 40 feet. Each unit was equipped with a single-station battery-operated smoke detector. Unfortunately, the battery of the smoke detector in the apartment of origin had been removed. There were no sprinklers.

The local fire department received notification of the fire at 8:00 p.m., and fire officials believe there was little delay in reporting. After a delay in access due to the security devices described below, first-arriving units forced entry. They eventually knocked down the fire and located the victims' bodies.

Two of the three victims had attempted to escape from the apartment but were found at the front door, which had a double-cylinder locked screen door of heavy steel. Security bars blocked all windows. News accounts reported that neighbors were able to see the father, with one child in his arms, attempt unsuccessfully to escape.

Single-Family Dwelling

Two Die When Security Bars Prevent Escape; South Carolina, July 1985

Children playing with matches in a bedroom started a fire that damaged their house and killed their 74-year-old great-grandmother and the 8-year-old boy who was probably responsible for the blaze.

The house, which measured 40 by 25 feet, was one story high with concrete-block walls, a wood floor, and a wood roof assembly covered with asphalt shingles. Its windows were fitted with steel security bars, and the front and rear doors were equipped with steel guard doors. The yard around the house was enclosed by a chain link fence, and the house itself had no smoke detectors or fire extinguishers.

Two brothers, ages 8 and 5, and their 4-year-old sister were in a bedroom playing with matches and a candle when the bedding ignited. The children left the room, leaving the door open, and tried to escape from the house, apparently without notifying their great-grandmother, who was babysitting. The two youngest unlocked the rear security door with the only key available and fled the building. The oldest child and the woman were trapped inside the burning house when they were unable to open the doors or windows.

US Coast Guard Communications Center Alaska, September 23

This large-loss fire severely damaged a Coast Guard communications center that monitored incoming distress signals for the North Pacific.

The two-story communications center, which measured 96 by 52 feet, was of reinforced concrete construction with wooden roof decking and a built-up asphalt roof covering. The building contained just two windows, both on the first floor, and had no automatic detection or sprinkler systems. At the time of the fire, the facility was only partially operational, with one man on duty.

At approximately 2:44 am, the man standing watch notified the fire department of an intense accumulation of smoke in the secured facility. First-arriving fire units found heavy smoke coming from the first-floor window on the north side of the building, but they were unable to get into the secured areas of the building because the doors were locked with a dead bolt and combination locking system to which the man on watch did not know the combination. To reach the fire, firefighters had to operate their handlines through the broken windows. They eventually extinguished the blaze at 3:45 am and entered the building through the north window to perform overhaul operations.

Investigators determined that the fire began when a communications machine short-circuited and caused a slow build-up of heat which ignited surrounding combustibles.

The fire resulted in a loss of \$1.5 million.

Item	NFPA 101 - 1991	BOCA - 1990
1. Minimum Exit Width for corridors and aisles	44" for corridors and passageways in new and existing buildings (sections 26-2.3.2, 27-2.3.2); 36" for all other exit access components in new buildings and 28" in existing buildings (section 5-3.4.1)	44" when serving > 50 persons; 36" when serving < 50 persons (section 810.3)
2. Maximum Travel Distance (Exit Access)	200' for an unsprinklered building; 300' for a building sprinklered throughout (sections 26-2.6, 27-2.6)	200' for an unsprinklered building; 250' for a building sprinklered throughout (section 807.5)
3. Maximum Corridor Dead-End Limit	20' for new, unsprinklered buildings; 50' for new, sprinklered buildings; 50' for existing buildings (sections 26-2.5.2, 27-2.5.5)	20' (section 810.2)
4. Maximum Common-Path-Of-Travel	75' for unsprinklered buildings; 100' for sprinklered buildings; 100' for single tenant spaces with an occupant load of \leq 30 persons (sections 26-2.5.3, 27-2.5.3)	Not Specified by BOCA
5. Number of Exits from a room or tenant space	Determined Indirectly by Common Path of Travel requirement	2 exits or exit access doors required from every room or space except when the maximum travel distance from the most remote point within the space to a single exit access door does not exceed 75' and the number of persons within the space at no time exceeds 50. (section 813.2)
6. Remoteness of Exits	When two or more exits are required from a space or building, at least two of the exits shall be separated by a distance equal or greater to 1/2 the maximum diagonal of the space served, or 1/3 the diagonal if the building is sprinklered. (section 5-5.1.4)	When two or more exits are required from a space or building, at least two of the exits shall be separated by a distance equal or greater to 1/2 the maximum diagonal of the space served, or 1/4 the diagonal if the building is sprinklered. (section 807.4.1)

Item	NFPA 101 - 1991	BOCA - 1990
7. Locking of Stairwell Doors	<p>All interior means of egress stairway doors shall allow reentry from the stairway, or an automatic release shall unlock all stairway doors. (section 5-2.1.5.2)</p> <p>Selected doors may be locked against reentry. (section 26-2.2.2.3)</p> <p>Reentry not required for existing buildings (section 27-2.2.2.5)</p>	<p>All interior stairway means of egress doors shall be openable from both sides w/o the use of a key or special knowledge. (section 817.11.3)</p> <p>Reentry may be locked if all doors are provided with special locking arrangements. (section 813.4.1.2)</p>
8. Panic Hardware Required	<p>No</p>	<p>No</p>
9. Exit Door Locking Hardware Restrictions	<p>Doors shall be readily openable in the direction of egress with no more than one releasing action and without the need of a special key, tool, or knowledge. (section 5-2.1.5.1)</p> <p>The principal exterior entrance/exit doors are permitted to have key operated locks provided the doors are unlocked when the building is occupied (accessible to public or occupied by 10 or more persons [section 5-2.1.1.3]), a key is available to any occupant inside the building when it is locked, and the device is readily distinguished as locked. (sections 26-2.2.2.2, 27-2.2.2.2)</p> <p>Special locking arrangements may be provided. (sections 26-2.2.2.4, 27-2.2.2.4)</p> <p>Security grills are permitted on egress doors provided that they remain full open when the space is occupied and they shall be readily openable from the egress side without the use of any special knowledge or effort. (sections 26-2.2.2.5, 27-2.2.2.5)</p>	<p>All means of egress doors shall be readily openable from the side from which egress is to be made without the use of a key or special knowledge or effort. (section 813.4.1)</p> <p>The principal exterior entrance/exit doors are permitted to have key operated locks provided the doors are unlocked when the building is occupied and the device is readily distinguished as locked. (section 813.4.1 exception 6)</p> <p>Manually operated edge or surface mounted deadbolts are prohibited. (section 813.4.1.1)</p> <p>Maximum 1 special locking arrangement allowed. (section 813.4.1.2)</p> <p>Security grills on egress doors shall remain open during occupancy by the general public, may not be closed when more than 10 persons occupy a space served by a single exit or 50 persons in spaces served by more than one exit. Not more than half of the required exits may be equipped with grills. (section 813.5)</p>

DCID 1/21 Quick Reference Guide (In U.S.)

SCIF	Location	Storage	Controlled	Construction	IDS Response
Proposed SCIF In U.S.	Above Ground Floor	Open 3.1.2	Compound	Dry Wall	5 Min
			Building		
			Office		
	Closed 3.1.1	Compound	Dry Wall	15 Min	
		Building			
		Office			
	Ground Floor **	Open 3.1.2.1c	Compound	Dry Wall **	5 Min
			Building	Ex Metal **	
Office			Ex Metal/Vault		
Closed 3.1.1.1e		Compound	Dry Wall **	15 Min	
Building					
Office					

* Window protection required.

** Exterior wall may require additional protection.

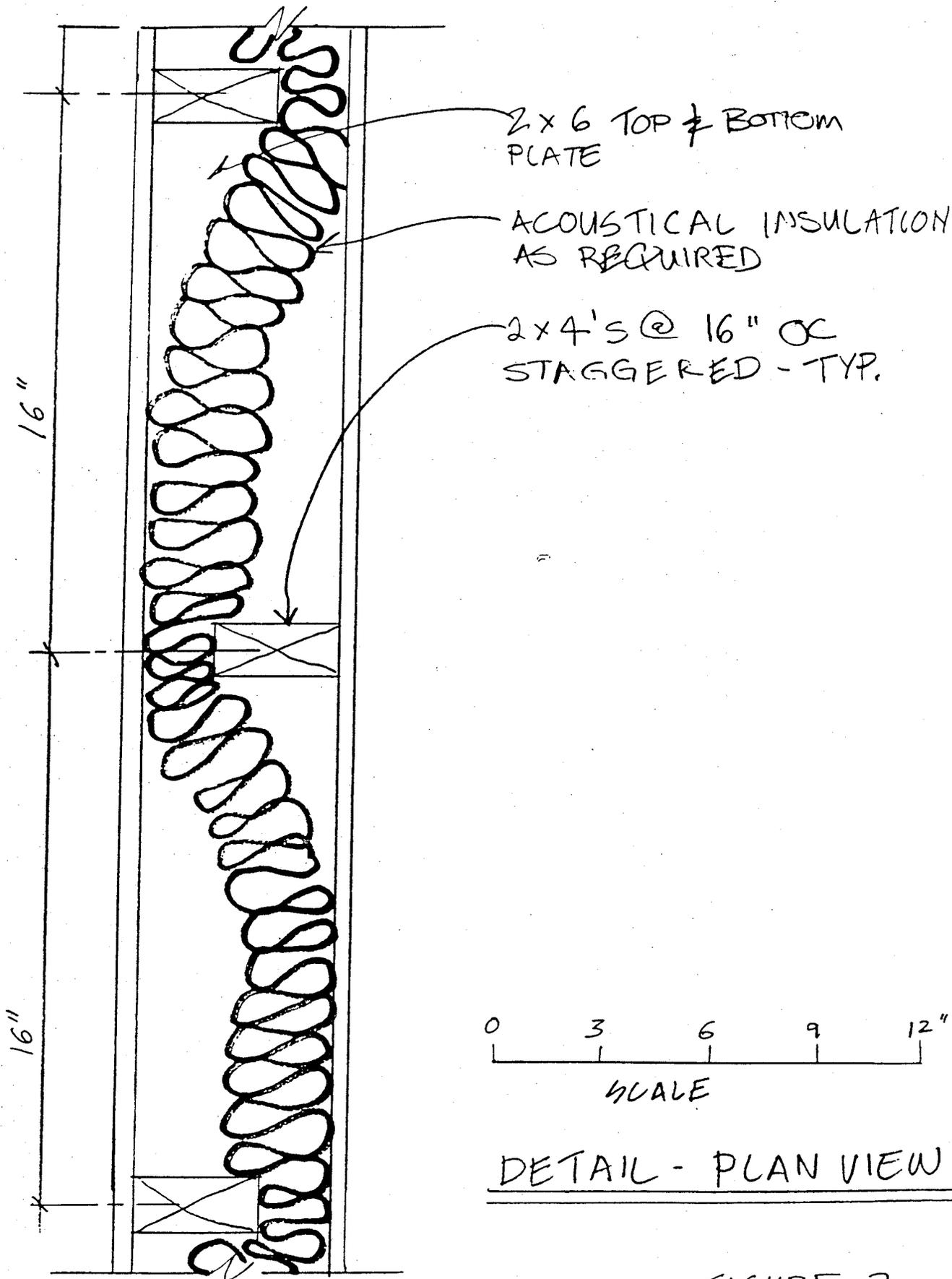


FIGURE 2

Basic Types of SCIF Doors

- Primary Entrance
 - Combination Lock conforming to Federal Specification AA-D-00600, Dec. 1 1990
 - Unican 1000
- Secondary Entrance
 - Unican 1000
 - Sliding deadbolts
- Emergency Exit Only
 - Alarmlock Model 700 Panic Exit Deadbolt,
- Communicating Door-Convenience
 - Sliding deadbolts, both sides
- Communicating Door-Required Exiting
 - Non-locking passage set

SUBMITTAL REGISTER														CONTRACT NO.					
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001										CONTRACTOR									
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY					MAILED TO CONTR/ DATE	REMARKS		
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REV/	DATE RCD FROM OTHER REV/	ACTION CODE	DATE OF ACTION				
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)	(q)	(r)		
		01020	SD-01 Preconstruction Submittals																
			Contractor's Environmental Coordinator	3.01	G														
			Storm Water Pollution Plan	3.04	G														
			Ohio EPA Form	3.05	G														
			Recycling and Solid Waste	3.07	G														
			Site Specific Spill Plan	3.08	G														
			Hazardous Material Paragraph B	3.09	G														
			Hazardous Material Paragraph C	3.09	G														
			Hazardous Waste	3.10	G														
			Resource Conservation Recovery	3.10	G														

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER															CONTRACT NO.		
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001										CONTRACTOR							
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY					MAILED TO CONTR/ DATE	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVI	DATE RCD FROM OTHER R	ACTION CODE	DATE OF ACTION		
			Hazard Communication Plan	3.09	G												
	01451		SD-01 Preconstruction Submittals														
			Quality Control Plan	3.2	G, RE												
	02081		SD-01 Preconstruction Submittals														
			Precise Site Drawings		G												
			Scaled Site Drawing		G												
			Regulated Area		G												
			Hygiene Facilities		G												
			Negative Pressure and Air Flow Patterns		G												
			Critical Barriers		G												
			ACM Locations		G												

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER										CONTRACT NO.					
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001										CONTRACTOR					
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY			MAILED TO CONTR/ DATE	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVI	DATE RCD FROM OTHER R		
			Regulated Area		G										
			Asbestos Related Blueprints		G										
			Asbestos Abatement Ohio License		G										
			Asbestos Abatement Ohio Certification Specialist		G										
			Asbestos Abatement Ohio Worker Certification		G										
			Asbestos Evaluation Certification		G										
			Industrial Hygienist Certification		G										
			Testing Laboratory Certification		G										
			EPA Approved Landfill		G										
			Exposure Monitoring		G										
			Air Sampling		G										

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER										CONTRACT NO.						
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001										CONTRACTOR						
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY				MAILED TO CONTR/ DATE	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVI	DATE RCD FROM OTHER R	ACTION CODE		
			Asbestos Abatement Plan		G											
			Proposed Method to Maintain Temperatures		G											
			OEPA and ODH Notifications		G											
			Employee Training		G											
			Respirator Training		G											
			Medical Surveillance		G											
			Emergency Procedures		G											
			Insurance Certificate		G											
			Laboratory Quality Control		G											
			Complete List of Employees		G											
			Form 1414		G											

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER										CONTRACT NO.					
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001										CONTRACTOR					
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY			MAILED TO CONTR/ DATE	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REV/	DATE RCD FROM OTHER R/		
			SD-13 Records												
			Background, Personal, etc.		G										
			Daily Inspection Checklists		G										
			Air Pressure Differential Strip Chart		G										
			Asbestos Containing Waste Manifest		G										
			Post-Abatement Submittal		G										
	02083C		SD-13 Records												
			Form 1438		G										
	02083D		SD-01 Preconstruction Submittals												
			Removal Start Date		G										
			SD-13 Records												

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER										CONTRACT NO.					
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001										CONTRACTOR					
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY			MAILED TO CONTR/ DATE	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVI	DATE RCD FROM OTHER R		
			Form 1438		G										
	02090		SD-01 Preconstruction Submittals												
			Job-Specific Plan	1.07.1	G										
			Site-Specific Work Plan Checklist	1.07.6	G										
			Permits and Notifications	1.08	G										
			Notification Prior to Work	1.10.1	G										
			SD-06 Test Reports												
			Monitoring Results	1.09.1	G										
			SD-13 Records												
			Bill of Lading	1.09.3	G										
			Laboratory Analytical Reports	1.09.3	G										

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER											CONTRACT NO.						
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001											CONTRACTOR						
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY					MAILED TO CONTR/ DATE	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVI	DATE RCD FROM OTHER R	ACTION CODE	DATE OF ACTION		
		02091	SD-01 Preconstruction Submittals														
			Work Plan		G												

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER																CONTRACT NO.	
Title and Location						CONTRACTOR											
FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001																	
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR /	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY					MAILED TO CONTR/ DATE F	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVIE	DATE RCD FROM OTHER RE	ACTION CODE	DATE OF ACTION		
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)	(l)	(m)	(n)	(o)	(p)	(q)	(r)
		08346	SD-02 Shop Drawings														
			Doors		G												
			Frames		G												
			Accessories		G												
			Sound Striping		G												
			Schedule of Doors		G												
			Schedule of Frames		G												
			SD-03 Product Data														
			Doors		G												
			Frames		G												
			Sound Striping		G												
		10550	SD-03 Product Data		G												
			SD-02 Shop Drawings		G												
		16750	SD-03 Product Data														
			Manufacturer's Product Data Sheets		G												
			SD-02 Shop Drawings														

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.

SUBMITTAL REGISTER											CONTRACT NO.					
Title and Location FY2003, ALTER GRAD ED FAC WPAFB ***SAFETY PAYS*** ZHTV013001					CONTRACTOR											
ACTIVITY NO	TRANSMITTAL NO	SPEC SECT	DESCRIPTION ITEM SUBMITTED	PARAGRAPH #	CLASSIFICATION GOVT OR /	CONTRACTOR SCHEDULE DATES			CONTRACTOR ACTION		APPROVING AUTHORITY				MAILED TO CONTR/ DATE F	REMARKS
						SUBMIT	APPROVAL NEEDED BY	MATERIAL NEEDED BY	ACTION CODE	DATE OF ACTION	DATE FWD TO APPR AUTH/	DATE FWD TO OTHER REVIE	DATE RCD FROM OTHER RE	ACTION CODE		
			Shop drawings for the installation		G											
			SD-10 Record Drawings													
			Record Drawings		G											
			Operation and Maintenance Manuals		G											

NOTES:

1. Closet rod product data.
2. Installation instructions.
3. Type of welding.
4. Operation and maintenance instructions.
5. Performance test results.