

FOR OFFICIAL USE ONLY

Department of Homeland Security

Special Programs Security Division (SSPD)

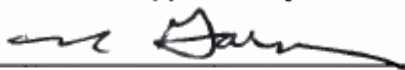
Accreditation and Technical Support Branch (ATSB)



SENSITIVE COMPARTMENTED INFORMATION FACILITY (SCIF) STANDARD CONSTRUCTION & DESIGN PACKAGE

August 2007

Issued and Approved By:

 8/16/07

Ken Garner
Chief, Special Security Programs Division
Department of Homeland Security

Date

Office of Security
Washington DC 20528



**Homeland
Security**

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

CHANGE PAGE	IV
INTRODUCTION.....	VI
PURPOSE.....	VII
AUTHORITIES.....	VIII
DEFINITIONS	IX
ADMINISTRATIVE PROCEDURES.....	1
SCIF ACCREDITATION REQUIREMENTS.....	1
CONCEPT AND PRECONSTRUCTION APPROVAL	1
THE FIXED FACILITY CHECKLIST (FFC)	1
CONSTRUCTION REQUIREMENTS AND SPECIFICATIONS	2
HANDLING AND DISTRIBUTION OF DRAWINGS	2
CONSTRUCTION STANDARDS	3
MILEPOSTS FOR INSPECTION	3
GENERAL NOTES.....	4
EXPANDED METAL MESH SPECIFICATIONS	6
SCIF PERIMETER WALLS	7
SCIF DOORS.....	7
PRIMARY ENTRANCE DOOR	8
SECONDARY ENTRANCE DOORS.....	9
SCIF EMERGENCY EXIT DOOR	9
DIELECTRIC BREAKS	10
DUCTS	10
TECHNICAL SECURITY	11
TELEPHONE SECURITY	11
COMPUTERIZED TELEPHONE SYSTEMS (CTS)	11
RF ATTENUATION & TEMPEST MITIGATION.....	12
RF WINDOW FILM SPECIFICATIONS.....	12
SOUND ATTENUATION.....	14
STC RATINGS	14
TESTING PROCEDURES	14
WINDOWS	15
ACCESSIBLE WINDOWS.....	15
INTRUSION DETECTION SYSTEM (IDS).....	16
ALARM COVERAGE.....	16
DATA / TELEPHONES / POWER.....	17
DEDICATED POWER PANEL	17
DEDICATED GROUND.....	17

COMPUTER EQUIPMENT ROOM (CER) SHUNT-TRIP BREAKER	17
UNINTERRUPTIBLE POWER SUPPLY (OPTIONAL UPS).....	17
TEMPEST FILTERING.....	18
HVAC COMPUTER EQUIPMENT ROOM (CER) REQUIREMENTS.....	18
HVAC AIR CONDITIONING.....	18
TEMPERATURE ADJUSTMENTS.....	18
HUMIDITY RANGE	18
AIR SUPPLY DISSIPATION	19
AIR HANDLER LOCATION.....	19
COMMUNICATION LINE INSTALLATION.....	19
CONVEYANCE SYSTEMS INSTALLED IN CEILINGS	19
RED CONVEYANCE SYSTEMS UTILIZING WIRE.....	19
ACCESSIBILITY.....	19
CONVEYANCE BENDS.....	19
CONVEYANCE SYSTEMS BETWEEN SCIFS.....	20
PROTECTED DISTRIBUTION SYSTEM(S) (PDS).....	21
PROTECTED DISTRIBUTION SYSTEMS (PDS) APPROVAL REQUEST	22
CONNECTIVITY GUIDELINES / GENERAL SPECIFICATIONS	24
COMMERCIAL DEMARCATION	24
WIDE AREA NETWORK(S) (WAN) CONNECTIVITY.....	24
SECURE VIDEO TELECONFERENCING	24
NON-SECURE (BLACK) WALL PLATES (VOICE AND DATA).....	25
NON-SECURE VOICE CABLE DISTRIBUTION.....	25
SECURE (RED) WALL PLATES (VOICE AND DATA)	26
SECURE VOICE CABLE DISTRIBUTION (TDM).....	26
SECURE VOICE CABLE DISTRIBUTION (IP)	26
INFRASTRUCTURE CABLING.....	26
STANDARD WALL DESIGNS / DUCT DETAILS / FIGURES.....	27
WALL TYPE 1 - ACOUSTICALLY-TREATED PARTITION	28
WALL TYPE 2: - ACOUSTICALLY-TREATED PARTITION (STC-45).....	29
WALL TYPE 3A: - SCIF WALL PERIMETER WALL PARTITION.....	30
WALL TYPE 3B - SCIF WALL PARTITION ON PERIMETER WALL	31
WALL TYPE 4 - SECURE PERIMETER PARTITION.....	32
TRANSFER DUCT -Z-DUCT / PASSIVE AIR RETURN	33
MANBAR BARRIER.....	34
SECURITY BAR DETAIL	35
SECURITY GRILL/PERIMETER WALL ELEVATION DETAIL	36
SAMPLE - UL FIRE RATED / STC RATED / DOOR AND FRAME ASSEMBLY	37
SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT (FIBERPLEX)	38
SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT (PCT-FTX3R)	42
SUGGESTED FIRE ALARM ANNUCIATOR EQUIPMENT (HORN STROBE)	44
SUGGESTED FIRE ALARM ANNUCIATOR EQUIPMENT (SPEAKER ASSEMBLY)	45
SUGGESTED PUBLIC ANNOUNCEMENT (PA) SYSTEM EQUIPMENT	46
BEST PRACTICES	48

CHANGE PAGE

No.	CHANGE	CHANGE DATE
1.	ORIGINAL DOCUMENT RELEASE (ODR)	8-16-07
2.	Change page 9 & page 16, approved BMS types	8-30-2007
3.	Change administrative	9-10-2007
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		
20.		
21.		
22.		
23.		
24.		
25.		
26.		
27.		
28.		
29.		
30.		
31.		
32.		
33.		
34.		
35.		
36.		
37.		
38.		
39.		
40.		
41.		
42.		

FOREWORD

This handbook is issued under the authority of the Director Central Intelligence Directive (DCID) 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities" and The Department of Homeland Security, Management Directive 11043, "Sensitive Compartmented Information Program Management".

This handbook applies to the Department of Homeland Security (DHS), its Components (excluding the United States Coast Guard), Directorates, Offices, and Field Activities. References made in this handbook to DHS will be considered to include all Components (excluding the United States Coast Guard), Directorates, Offices, and Field Activities, and entities encompassed under the jurisdiction of the Homeland Security Act and amendments thereto. The United States Coast Guard maintains their designated membership in the Intelligence Community and will continue to manage and operate its own intelligence program.

This handbook also applies to contractors in SCI Facilities (SCIFs) accredited by the DHS and to DHS SCI contract efforts conducted within facilities accredited by other agencies and approved for joint use by co-utilization agreement.

Heads of DHS Intelligence Components may issue supplementary instructions when necessary, to address unique situations to meet mission requirements within their respective components. All supplementary instructions must be approved by the Cognizant Security Authority (CSA) prior to implementation. Provisions outlined in this handbook take precedence over previously issued legacy manuals, instructions, guidance and other publications.

Comments regarding and/or recommendations to change this handbook, should be directed to the DHS Security Office, ATTN: Special Security Programs Division (SSPD), Accreditation and Technical Support Branch.

INTRODUCTION

This handbook contains standard security designs and procedures common to Sensitive Compartmented Facilities (SCIF) and physical security construction standard and established by the Director National Intelligence (DNI) for protection of classified intelligence information. Users should refer to Director of Central Intelligence Directives (DCIDS) and other documents cited under Authorities for guidance on specific security functions.

PURPOSE

This handbook contains security procedures, and details for the construction of Sensitive Compartmented Information Facilities (SCIF) for the Department of Homeland Security (DHS). This handbook provides key milestones, construction standards, electrical and technical guidance for use when planning and executing the construction of DHS SCI Facilities (SCIFs).

This reference manual should be used as a guide for construction professionals, engineers, architects, Special Security Officers and project managers to ensure the required construction standards are established and meet DHS and DCID minimum requirements.

Adherence to this guide will assist in facility accreditation in accordance with DCID 6/9 standards.

DHS Facilities Division, construction professionals, engineers, architects, Special Security Officers and project managers should verify their design intent and concept of operation through the Cognizant Security Authority (CSA) prior to entering into a DHS SCIF construction project.

Approval of a SCIF Concept of Operations (CONOPS) is critical to the facility accreditation and should be the initial documentation established prior to beginning, planning and or construction of an SCI facility.

Make all CONOPS approval requests through the Office of Security, ATTN: Special Security Programs Division, Chief Security Officer.

AUTHORITIES

1. The Homeland Security Act of 2002, P. L. 107-296
2. The National Security Act of 1947, 50 U.S.C. 401
3. Executive Order 12333 "United States Intelligence Activities"
4. Executive Order 12829, "National Industrial Security Program"
5. Executive Order 12958, as amended, "Classified National Security Information"
6. Executive Order 12968, "Access to Classified Information"
7. Executive Order 13284, "Establishment of the Department of Homeland Security"
8. Director of Central Intelligence Directive (DCID) 6/1, "Security Policy for Sensitive Compartmented Information and Security Policy Manual"
9. DCID 6/3, "Protecting Sensitive Compartmented Information Within Information Systems"
10. DCID 6/4, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information"
11. DCID 6/7, "Intelligence Disclosure Policy"
12. DCID 6/9, "Physical Security Standards for Sensitive Compartmented Information Facilities"
13. Department of Homeland Security Delegation Number 8000.1, "Delegation to Chief, Office of Security of Determination Authority and Cognizant Security Authority"
14. Designation of Chief Security Officer as Senior Agency Official, March 3, 2004
15. Department of Homeland Security Management Directive number 11043 Sensitive Compartmented Information Program Management

DEFINITIONS

A. Accreditation is 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.

B. Cognizant Security Authority (CSA) is the individual designated by a Senior Official of the Intelligence Community (SOIC) to serve as the responsible official for all aspects of security program management with respect to protection of intelligence sources and methods under SOIC responsibility. The CSA for DHS is the Chief Security Officer.

C. Contractor Special Security Officer (CSSO) administers the receipt, control, and accountability of SCI materials and the SCI security functions for contractor facilities.

D. Information System Security Manager (ISSM) The security official responsible for the IS security program for a specific Directorate, Office, or contractor facility.

E. Information System Security Officer (ISSO) The security official, either government or contractor, responsible for the security posture of a specific Information System.

F. Intelligence Community includes United States Government agencies and organizations and activities identified in the National Security Act of 1947.

G. National Foreign Intelligence Board is chaired by the Director of Central Intelligence and is comprised of Intelligence Community members and distinguished civilians appointed by the President.

H. Need-to-know is a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform a lawful and authorized function. Such person shall possess an appropriate security clearance and access approvals in accordance with Executive Orders 12958, as amended, and 12968, as well as DCID 6/4.

I. Senior Agency Official is the official designated by the agency head under section 5.4(d) of E.O. 12958, as amended, who directs and administers the agency's program under which information is classified, safeguarded, and declassified. The Senior Agency Official for DHS is the Chief Security Officer.

J. Senior Official of the Intelligence Community (SOIC) is the head of an organization within the Intelligence Community, as defined by the National Security Act of 1947. Within DHS there are five SOICs: The Secretary, the Deputy Secretary, the Under Secretary for Information Analysis and Infrastructure Protection, the Assistant Secretary for Information Analysis, and the Assistant Commandant for Intelligence for the United States Coast Guard.

K. Sensitive Compartmented Information (SCI) is classified information concerning, or derived from, intelligence sources, methods, or analytical processes requiring handling within formal access control systems established by the Director Central Intelligence (DCI). SCI is also referred to as "codeword" information. The sensitivity of this information requires that it be protected in a much more controlled environment than other classified information. Therefore, the DCI has established special policies and procedures for the protection of SCI. These policies and procedures are promulgated through Director of Central Intelligence Directives (DCIDs).

L. SCI Facility (SCIF) is an accredited area, room, group of rooms, buildings, or installation where SCI may be used, stored, discussed and/or processed.

M. Security Clearance is a formal authorization for an employee with a specific need-to-know to have access to information that is classified as Confidential, Secret, or Top Secret in the interest of national security or the defense of the United States.

N. Special Security Officer (SSO) works under the direction of the Chief, Special Security Programs Division and administers the receipt, control and accountability of SCI. The SSO oversees SCI security functions and reporting requirements for subordinate SCIFs.

O. Special Security Representative (SSR) works under the direction of the supporting SSO, and is responsible for the day-to-day management and implementation of SCI security and administrative instructions for a separate, subordinate DHS SCIF.

P. Technical Surveillance Countermeasures are techniques and measures used to detect and nullify a wide variety of technologies used to obtain unauthorized access to classified national security information, restricted data, and/or unclassified sensitive information.

Q. Telecommunications and Automated Information Systems (TAIS) is defined as any telecommunications or computer related equipment, or interconnected system or subsystems of equipment, that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice or data (digital or analog), including software, firmware, and hardware.

R. TEMPEST: Telecommunications Electronics Material Protected from Emanating Spurious Transmissions or Transient Electromagnetic Pulse Emanation Standard. Refers to external electromagnetic radiation from data processing equipment and the security measures used to prevent them.

ADMINISTRATIVE PROCEDURES

SCIF ACCREDITATION REQUIREMENTS

The Special Security Programs Division (SSPD) under authority of the Chief Security Officer (CSO) is the sole accrediting authority for DHS SCIFs. Divisions are responsible for ensuring SCIFs are established only when clear operational requirements dictate, and when existing SCIFs are not adequate to support the requirements. A clear, active SCI mission must exist before a SCIF is requested. SCI will not be discussed or introduced into the proposed SCIF until the facility is formerly accredited by SSPD. SCIF accreditation involves two basic steps: Concept and preconstruction approval, and Accreditation.

CONCEPT AND PRECONSTRUCTION APPROVAL

The concept approval step is a key element in future accreditation actions. Concept of Operations (CONOPS) approval certifies that clear operational requirements exist for the SCIF and there is no existing SCIF to support the requirement. Upon receipt of the CONOPS approval, the Directorate or Component Special Security Officer (SSO) will coordinate directly with SSPD on all matters pertaining to physical security/TEMPEST and accreditation of that SCIF. The SSO will send an information copy of any documentation to the appropriate Division Head. Divisions will not impose procedures which hinder this process. The CONOPS approval request, via Memorandum, will include the exact location of the proposed SCIF (Street Address and City); required level of SCI accesses (SI/TK/G/HCS, etc.); the storage requirement (Closed Storage, Open Storage or Continuous Operations (24/7 operations) and brief description of operation.

The DHS Chief Security Officer, or designee, is authorized to grant concept approval to establish a SCIF and to validate the requirement for the requested level of SCI. The CSO or designee will issue a concept validation (CONOPS) approval Memorandum to the requesting organization, with an information copy to the supporting SSO.

The SCIF design will balance threats and vulnerabilities against appropriate security measures to reach an acceptable level of risk. Proper security planning for a SCIF is intended to deny foreign intelligence services and other unauthorized personnel the opportunity for undetected entry into these facilities and exploitation of sensitive activities.

THE FIXED FACILITY CHECKLIST (FFC)

This is the primary document in the decision making process for granting an accreditation. The preconstruction FFC must describe in sufficient detail the types and methods of construction to determine if the SCIF construction will satisfy physical security criteria listed in DCID 6/9. Complete (to the extent possible) and submit the preconstruction FFC for the proposed SCIF along with a drawing of the space and the CONOPS request to SSPD. SSPD will review physical security preconstruction plans

for SCIF construction, expansion, or modification and will provide preconstruction advice, assistance, and formal written approval. Construction will not begin until SSPD provides formal preconstruction approval to proceed with construction.

CONSTRUCTION REQUIREMENTS AND SPECIFICATIONS

Prior to SCIF construction, SSPD must be provided with a copy of all preconstruction drawings for approval. Based upon a threat analysis, additional technical or physical enhancements may be required. Upon receipt of the drawings, SSPD will provide a written concurrence/non-concurrence within ten working days.

HANDLING AND DISTRIBUTION OF DRAWINGS

Drawings should be considered and marked For Official Use Only and handled in accordance with The Freedom of Information Act, The Intelligence Authorization Act of 2002 amending the FOIA and Privacy Act requirements accordingly.

Where possible drawings should be sanitized and a separate key document should be maintained by authorized personnel providing detailed description of rooms, mechanical and electrical details.

Drawings should have limited information regarding the activity or agency occupying the SCIF, etc. Drawings should reference all rooms by number with a separate key reference maintained separate from the drawing describing the room and requirements.

Drawings shall limit any indication(s) of function(s) or mission(s) of the facility.

Drawings shall not use the term (SCIF). As an alternative, another name, coding system or number should be assigned at the discretion of the facilities project manager and with concurrence from SSPD to identify SCI rooms and facilities.

CONSTRUCTION STANDARDS

MILEPOSTS FOR INSPECTION

Special Programs Security Division (SSPD) or Cognizant Security Authority (CSA) assigned representative must inspect the construction points described below.

1. During wall construction, but before its completion, all wall layers need to be inspected.
2. Following installation/welding of expanded metal in walls, but before walls are covered in sheetrock.
3. Following the installation of any duct grills, non-conductive breaks, or inspection ports.
4. Following any modification to seal cable trays (e.g. welding plates; installation of grill etc.) but before the tray is sealed.
5. Inspection of doors and hardware as specified, i.e. once doors are hung and all equipment is installed to include door sweeps, thresholds, and gaskets.
6. Final inspection to include confirmation of wall-to-ceiling (slab-to-slab) construction; complete sealing around all penetrations in perimeter walls, completion of walls above false ceiling in a workman-like manner to include painting both sides, and complete labeling of both ends of all telephone, fiber, and electrical circuits, to include all wiring and conveyance methods.

Many of these items shown above will be inspected at the same time, e.g. penetrations requiring dielectric breaks will be inspected as available at the same time that the expanded metal installation is inspected.

Ceiling tiles will not be installed until after the final inspection, so as to facilitate access to the plenum, and prevent damage to the tiles.

**** Every element of SCIF perimeter wall(s) installation must be made available for inspection by the government representative prior to concealment. ****

CONSTRUCTION STANDARDS

GENERAL NOTES

1. Building owner shall coordinate with government representative to obtain final tenant approval and acceptance of build-out. This may not be applicable in all locations, i.e. NAC facilities.
2. Any openings greater than 96 square inches in cross sectional area that penetrate any demising or perimeter wall must have a grill barrier unless the government representative (SSPD) certifies the opening is not man-passable. All grillwork frames shall be visible from the exterior of ductwork. A 12" X 12" (approximate) lockable access port shall be installed to permit periodic inspection of the grill. The access port shall allow visual and physical inspection of the grill or man-bar installation. All access ports shall be on tenant (secure) side of wall, and positioned such that access is not restricted. The actual size of the access port may vary, but shall be no less than 9" X 9" square. Tenant approval is required.
3. All existing wiring penetrating tenant spaces shall be removed or relocated. The only wiring approved to penetrate tenant space shall be wiring that is required by building code, or for tenant use. Remaining wiring will be labeled for identification. All wire penetrations shall be in conduit (unless otherwise dictated by code) and approved by the government representative (SSPD).
4. All abandoned equipment and conduit must be removed. Contractor shall fill voids with tenant-approved method.
5. All conduit or trough systems that penetrate perimeter walls, floors, or ceilings shall be fitted with dielectric (non-conductive) breaks, and must be on tenant (secure) side beginning within 6" of walls, floors, or ceilings, and should be no longer than 6". If this cannot be accomplished, SSPD will review and provide recommendations for mitigation of piping, fire systems, conduit or other penetrations, i.e., single point grounding, wrapping, isolation or isolated grounding.
6. Any trough system below floor or above ceiling shall be sealed, and the government representative (SSPD) shall approve both the method and type of seal.
7. Government project manager shall perform a final acceptance and inspection before the space is released for occupancy.
8. It is recommended that a Special Programs Security Division (SSPD) or Cognizant Security Authority (CSA) assigned representative be present with project manager during final acceptance inspection.

CONSTRUCTION STANDARDS

GENERAL NOTES

9. Contractor shall coordinate directly with government representative regarding location of existing and proposed mechanical penetrations and man-bar (grillwork) installation. **Coordination shall occur prior to any mechanical system procurement.**
10. All demising wall penetrations shall be reviewed and approved by government security representative (SSPD) and shall have non-conductive breaks. If this cannot be accomplished, SSPD will review and provide recommendations for mitigation of piping, fire systems, conduit or other penetrations, i.e., grounding, wrapping, or isolation.

CONSTRUCTION STANDARDS

EXPANDED METAL MESH SPECIFICATIONS

1. Expanded metal mesh shall meet ASTM F1267-89 type, Class 1 standard and shall have the following characteristics:
 - a. Strand thickness: No. 9 - 10 gauge minimum (flattened)
 - b. Weight: 195 lbs/csf minimum
 - c. Material: Carbon Steel
 - d. Shape: Flattened
 - e. Pattern: Diamond
 - f. Dimensions: 3.20 inch maximum (long opening) (LWD) 1.33 inch maximum (short opening) (SWD)
 - g. Recommended mesh: 3/4" #9 (10 ga)
2. Mesh shall be fastened to steel stud and top and bottom runners using either screw or weld attachment. Screws or weld shall be spaced at 6" on center maximum, with all corners fastened to the framing. Mesh splice shall occur at studs only. Splice between supports is not permitted unless: a) such splice is welded continuously top to bottom; b) mesh is overlapped three inches, and fastened or welded every six inches.
3. Steel framing receiving metal mesh shall be 16 gauge minimum.
4. Screws shall be self-drilling #8 shank minimum (1/4" minimum penetration into steel framing.) Fasteners must be used from the secure side of the mesh. 1/2 inch washers must be installed when using screws to deter ability to pull mesh over tops of screw heads.
5. Welds shall be 1/8" x 1/2" long fillet type excepting at unsupported splices where the weld must be continuous.
6. There can be no gap in coverage. Gaps may be closed with steel studding or flat metal welded (or fasted where welding is not permitted) to the secure side of the expanded metal.
7. A determination for use of expanded metal within SCIF walls will be made based upon threat assessment, facility type, government owned vs. leased, location as well as other factors.
8. The Nebraska Avenue Complex (NAC) has a waiver for metal mesh requirements for SCIF construction.

CONSTRUCTION SPECIFICATIONS

Prior to SCIF construction, SSPD must be provided with a copy of all preconstruction drawings for approval. Based upon a threat analysis, additional technical or physical enhancements may be required. Upon receipt of the drawings, SSPD will provide a written concurrence/nonoccurrence within ten working days.

SCIF PERIMETER WALLS

Perimeter walls must be true floor to true ceiling, finished and painted. Perimeter walls will be constructed in the following manner:

1. On the interior (secure side) of the perimeter wall, install one layer expanded metal mesh, standard flattened with diamond pattern, carbon steel with minimum flattened thickness of .120 inches (i.e., $\frac{3}{4}$ inch # 9 – 10 gauge mesh). The maximum dimensions of the long opening are 2.1 inches (80 millimeters) and the short opening is .923 inches (34 millimeters). Secure mesh to the metal framing via welding or with self-tapping #8 shank pan head screws at 6 inch (150 millimeters) on center maximum horizontally and vertically and a minimum of 7 millimeters penetration into the metal framing. Washers will be used to ensure secure fastening. Reference expanded metal mesh requirements for weld and installation instructions.
2. The interior (secure side) of the perimeter wall must consist of two layers 5/8 inch drywall mounted, on top of the metal mesh, on 16 gauge metal studs @ 16 inches O.C.
3. For perimeter walls that are adjacent to exterior building walls composed of substantive material, CMU, concrete block, steel, brick, etc., one layer of drywall may be eliminated. Reference wall detail type 3A and type 3B of this document.
4. Install a layer of 3 ½ inch sound batting or mineral wool material in the wall cavity. This construction method should provide a sound attention level of sound transmission class (STC) rating of 45 or greater.
5. On the exterior (non-secure side), install one layer of 5/8 inch drywall, with staggered seams, horizontally and vertically. Drywall should be staggered when using foil backed drywall. Drywall staggering is not required when using a foil barrier stapled between the two layers of drywall.

SCIF DOORS

Doors and frames shall meet or exceed an STC 45 rating at a minimum. The entire door, frame, partition, and door hardware assembly shall be designed and specified by the A/E firm to ensure the required STC rating is achieved.

Additionally, doors must meet a minimum forced entry requirement and be composed of a material that will withstand a forced entry attempt by

Doors will meet the following requirements:

1. Solid wood stave core door, a minimum of 1 ¾ inches thick, or
2. 16 gauge metal cladding over wood or composition materials, a minimum of 1 ¾ inches thick, or
3. Metal fire or acoustical protection doors, a minimum of 1 ¾ inches thick., or
4. 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.
5. All doors will be tested and meet a minimum Sound Transmission Class (STC) of 45. Install door sweeps, gaskets, astragal or overlapping molding to meet the STC-45 rating. All doors will have heavy duty automatic door closures.
6. If door(s) are equipped with hinges located on the exterior side of the door where it opens into an uncontrolled area outside of the SCIF, the hinge pins will be treated to prevent removal (e.g. pined, brazed, set screws, spot welded, etc.).
7. The non-active door of a double door configuration must be secured at the top (door jam) and bottom (floor) with heavy duty sliding deadbolts. Install heavy duty throw bolts on the inactive leaf (type Sergeant and Greenleaf (S&G) SM 181 slide locks on top and bottom or equivalent heavy duty slide bolts).
8. Use of wireless door opening devices is prohibited on garage doors. Remote door release devices are also prohibited unless approved in advance by the SSPD.
9. Install a UL 634 compliant (level 2) Balanced Magnetic Switch (BMS) which contains three or more balanced magnetic switches. A BMS is required on all doors that make up and or are apart of the SCIF perimeter boundaries/walls.

PRIMARY ENTRANCE DOOR

There will be one designated primary entrance door, unless approved in advance in writing from the CSO, Office of Security. The primary door must be equipped with a DHS installed GSA-approved combination lock (X09), an electric door latch rated at 2000 lbs force entry, and one-way door peep viewing port.

The door must have high security locking hardware (Medeco, Schlage Primus, Assa or similar approved hardware) that can override the access controlled electric door latch. Locking hardware shall meet UL 437 standards. The primary entrance door must be equipped with an automatic door closer and a dual access control device (key pad with

PIN and proximity card), in addition to the currently installed GSA-approved combination lock (X-09).

Install acoustical gasketing around the door and door sweeps to achieve an STC-45 sound rating. Reference Sound Attenuation.

SECONDARY ENTRANCE DOORS

These must be approved in advance by the SSPD. Secondary doors must be secured with approved deadlocking door hardware for securing the space after hours. The access control to this door must be disabled during periods of minimum staffing (6p.m. – 6a.m.). The keyway must be blanked on these doors.

SCIF EMERGENCY EXIT DOOR

The SCIF emergency exit door will be equipped with the following:

1. Deadlocking panic hardware (Von Duprin 9857-EO-F/9957-EO-F Three Point Latching Fire Device or similar) on the inside and have no exterior hardware.
2. Automatic door closer.
3. Balanced magnetic switch (BMS), Sentrol Model 2700 series, Harco Magnasphere HSD or equivalent (armed 24/7).
4. Local enunciator to alert personnel working in the area someone exited the facility due to emergency condition or other.
5. Install acoustical gasketing around the door and door sweeps to achieve and STC-45 sound rating.
6. Exposed hinges must be treated to prevent removal of the door (e.g., welded, set screws, etc).

CONSTRUCTION SPECIFICATIONS

DIELECTRIC BREAKS

DHS multi-tenant facilities must have non-metallic breaks on ducts, electrical conduits and water/sewer pipes that penetrate the SCIF perimeter. If this cannot be accomplished, SSPD will review and provide recommendations for mitigation of piping, fire systems, conduit or other penetrations, i.e., grounding, wrapping, or isolation.

DUCTS

Ducts over 96 square inches that penetrate the SCIF perimeter wall must have man bars installed at the point of entry. An inspection port must also be installed for visual verification and routine inspection on the secure side of the duct. Ducts with any dimensions less than 6" do not require man bars.

TECHNICAL SECURITY

TELEPHONE SECURITY

To prevent telephone lines and telephone instruments that service a SCIF from being used as clandestine listening devices, the following controls will be required:

1. All incoming telephone cables and wires which penetrate a facility's perimeter will enter the facility through one opening and be placed under control at the interior face of the perimeter by the following:

a. All active incoming lines will be accounted for by the number of pairs in use, by telephone and extension number, and the number of excess/unused pairs in existence. The accounting will be updated whenever the status of a pair of wires is changed.

b. All excess/unused incoming wires will be either removed or disconnected and grounded in a manner which prevents their unauthorized use.

2. The number of telephone instruments servicing a SCIF will be limited to those operationally necessary. All telephone instruments will be equipped with a non-resonating ringer, a positive disconnect either automatic or manual plug and jack, and, in certain installations a line filter. Specially designed, for U.S. Government use, telephone instruments and associated security devices are available from telephone companies. When planning the telephone system for a SCIF, advance consultation with SSPD is encouraged to obtain advice regarding recommended telephone instruments, associated security devices, installation design, and the required "certification of need" to obtain specially designed instruments and devices.

COMPUTERIZED TELEPHONE SYSTEMS (CTS)

Computerized telephone systems (CTS) or Voice Over Internet Protocol (VoIP) systems within the SCIF must meet Telephone Security Group (TSG) TSG-2 standards or utilize approved TSG type 6 equipment.

If the room is a "discussion area", all telephones installed in the space must be TSG-6 approved telephones, as an alternative, a TSG-2 configuration may be approved and utilized.

1. Administrative telephone systems are a potential source for fortuitous conduction of Compromising Emanations (CE) due to their proximity to building maintenance areas and their signal line distribution outside the facility. Additional protection is recommended when commercial telephones are located in a RED electromagnetic environment. The most effective protection is provided by line disconnection switches and telephone line optical isolators that use waveguide below cutoff. The use of these devices or telephone filters must be approved by

the CTTA. These devices should be considered only when installing, replacing or retrofitting telephone systems.

2. Remember that the administrative telephone system and its associated wiring are BLACK. The telephone system cabling should be routed in a separate distribution system. If filters or isolators are required and approved by the CTTA, the lines should be filtered/isolated where they egress the inspectable space or facility. Locating the filters/isolators at the controlled space is not recommended because the equipment TEMPEST zone may extend beyond the controlled space. In addition, fewer filters/, isolators will be necessary if the trunk lines rather than the individual phone lines are filtered/isolated.
3. CATV: Cable Television service into the SCIF must be electrically isolated at the point of entry. SSPD recommends the use of Fiber Plex Incorporated Uni-Directional (Simplex) Composite Video Optical Transmitter and Optical Receiver models (FOI-2170) and (FOI-2172) or similar isolation device also PCT International's 1310 nm Rackmount Transmitter (PCT-FTX3R) suitable for NTSC or PAL television signal transmission. Analog bandwidth to 870 MHz allows for advanced services such as HDTV, VOD, PPV, and high speed data as well as traditional cable TV.
4. Fire alarm horn strobes and horn enunciators installed inside of the SCIF will have a self amplified speaker configuration. Wheelock models SA-70 and SA-70s or similar device(s) are recommended.

RF ATTENUATION & TEMPEST MITIGATION

Based upon a threat determination and analysis of the proposed SCIF site, location and mission, RF Attenuation may be required. A determination will be made by SSPD prior to construction of the facility in accordance with CNSS 7000 and NSTISSI 7000, TEMPEST countermeasures for facilities, date May 2004. If a determination is made that TEMPEST countermeasures are required the following information is provided:

1. On the interior (secure side), on top of the metal mesh, install two layers of 5/8 inch foil back drywall, with staggered seams, horizontally and vertically.
2. The preferred method of RF mitigation is to install two layers of drywall: Install one layer of 5/8 inch drywall. Install a layer of TVM Ultra NT Radiant barrier foil (part # 1800 48 125s) or equivalent approved product. Seams must be overlapped and taped with metallic tape, or folded appropriately. Install a second layer of regular 5/8 inch drywall on top of the foil barrier.

RF WINDOW FILM SPECIFICATIONS

The following are the technical recommendations for all clear window film installed as an after market item. The preferred method is the film to be installed between the glazing as part of the window construction process prior to being placed in the window

frame.

1. Radio Frequency attenuation greater than or equal to: 30dB from 30MHz to 1.5 GHz.
2. Infrared attenuation greater than or equal to: 80% at 800 nm (nanometer) 90% at 900 nm 94% at 1000 nm 98% at 1550 nm - 2300 nm
3. Ultra Violet attenuation greater than or equal to: 70% at wavelengths less than 400 nm 90% at 375 nm 90% at 350 nm
4. Total visible (400nm – 780 nm) transmission greater Than or equal to 60%
5. Glazing system blast rated to GSA Glass Fragment Hazard Ranking 2. Can also be put within the PVB of the glass, (preferred and much cheaper).

The DHS only aware of two manufacturers that provide a window glazing product that meet or exceed these requirements, 3M and Signals Defense. DHS SSPD is available to review any other product that may be used in lieu of these suggested vendors.

SOUND ATTENUATION

Acoustical protection measures and sound masking systems are designed to protect discussion of classified information from being inadvertently overheard by the casual passerby. Secure Area and SCIF perimeter walls, doors, windows, floors and ceilings, including all openings, will provide sufficient sound attenuation to preclude inadvertent disclosure of conversation.

The ability of a Secure Area or SCIF structure to retain sound within the perimeter is rated using a descriptive value, the STC. All DHS Secure Areas and SCIFs will meet Sound Group III – STC of 45 or better. Higher levels are required for amplified sound (e.g., video teleconferencing).

STC RATINGS

Sound Group III – STC of 45 or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.

Sound Group IV – 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.

TESTING PROCEDURES

1. Procedures for measuring the sound attenuation levels of a completed structure can be found in, "Tentative Recommended Practices for Measurement of Airborne Sound Insulation in Buildings," Publication No. E-336-67T, American Society of Testing and Materials.
2. Another acceptable procedure is found in the DCI Security Committee memorandum, "Sound Attenuation Test for Secure Conference Rooms," dated 7 Feb 78.

WINDOWS

Where windows exist affording visual surveillance of personnel, documents, materials, or activities within the SCIF, the windows shall be made opaque or equipped with blinds, drapes, or other coverings precluding such visual surveillance. All accessible perimeter windows at ground level (less than 18 feet above the ground) shall be covered by an Intrusion Detection System (IDS).

ACCESSIBLE WINDOWS

This 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. roofs, fire escapes, electrical transformer, air conditioning units, vegetation or landscaping which can be climbed) will be constructed from or covered with materials which will provide protection from forced entry. The protection provided to the windows needs to be no stronger than the strength of the contiguous walls. Vertical Metal bars 1/2 inch thick, welded 6 inches on center will be installed on all accessible windows. Additional horizontal bars must be used to prevent spreading. As an alternative, Exeter, Level 5, or Kane Screens Level 5 (Crimeshield) or similar product may be used. Secure areas located within fenced and guarded government compounds with a 24/7 armed guard presence 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. In these instances, shock-type glass break sensors must be installed on accessible windows. All windows will be protected by Passive Infra-Red (PIR) motion sensors.

INTRUSION DETECTION SYSTEM (IDS)

An IDS must detect an unauthorized or authorized penetration in the secure area. An IDS complements other physical security measures and consists of Intrusion Detection Equipment, Security Forces and Operating procedures.)

IDS systems shall be installed in accordance with Annex B of the DCID 6/9.

ALARM COVERAGE

The facility will have adequate alarm coverage:

1. Install Sentrol Model 2700 series, Harco Magnasphere HSD or equivalent (armed 24/7) on all perimeter doors.
2. Install a UL 634 compliant (level 2) Balanced Magnetic Switch (BMS) which contains three or more balanced magnetic switches.
3. A BMS is required on all doors that make up and or are apart of the SCIF perimeter boundaries/walls.
4. Interior space must have full passive infrared (PIR) coverage.
5. Install alarm key pad inside the room, next to the primary entrance door.
6. Install alarm control panel inside the room or equipment closet.
7. IDS must be an independent system contained within the SCIF perimeter.
8. Alarm must be monitored by the DHS, FPS Mega Centers, or other UL 2050 Compliant monitoring station.
9. Alarm installer and monitoring location must be UL 2050 compliant.
10. Any wiring for the IDS or ACS penetrating the SCIF perimeter must be protected utilizing 128 bit encryption.
11. Access control to be provided with a electronic access control device.

IDS systems shall be installed in accordance with Annex B of the DCID 6/9.

DATA / TELEPHONES / POWER

DEDICATED POWER PANEL

Electrical power connected to the communication equipment must be controlled via a separate Power Distribution Unit (PDU). Within a SCIF / Computer equipment room a circuit breaker from a preexisting PDU, which meets CIO shunt-trip requirements may be utilized. The PDU will be dedicated to installed communication equipment located within the CER; no power shall be fed from this panel that would service anything outside the SCIF. Reference NSTISSI 7000 TEMPEST Countermeasures for Facilities and contact SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD) for additional guidance. The dedicated power panel shall be surfaced mounted on, or recessed in, an interior wall (IAW NEC) within the SCIF. The OCAO shall determine specific location of the dedicated power panel and PDU voltage/ampere requirements during planning phase.

DEDICATED GROUND

A dedicated ground conductor shall be provided. The dedicated ground installation from the SCIF power panel to the ground point shall conform to National Electric code (NEC) and local code requirements. The total resistance of the ground conductor (minimum #2 AWG stranded green copper wire) between the SCIF technical ground bus and the building ground point shall also conform to NEC and local code requirements. Reference NSTISSAM TEMPEST/2-95, Red/Black Installation Guidance and contact SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD) for additional guidance.

COMPUTER EQUIPMENT ROOM (CER) SHUNT-TRIP BREAKER

The dedicated power panel shall be equipped with a shunt-trip main circuit breaker. When activated, the shunt-trip eliminates power distribution to communications equipment within CER when temperature exceeds a set level. Equipment Cabinet Power Communication equipment cabinets shall be directly hard-wired to the CER dedicated power panel.

UNINTERRUPTIBLE POWER SUPPLY (OPTIONAL UPS)

Provides a degree of protection to attached equipment in the event of a short duration power outage. If communications requirements dictate UPS installation, any existing UPS may be utilized when placed prior to the CER PDU main power feed. However, when a communication equipment cabinet is protected by an individual UPS being supplied by CER PDU direct power, UPS will require ability to monitor the shunt-trip breaker connected to temperature thermostat and remove voltage distribution to protected equipment if a shunt-trip activation occurs. In the event customer determines they are unable to provide adequate UPS service to CER, OCIO engineer will evaluate, on a case-by-case basis, site requirements and determine if UPS unit(s) will be supplied to protect equipment contained within equipment cabinet(s).

**Uninterruptible Power Supply (UPS)
(For the protection of classified non-encrypted data processing)**

The APC Smart-UPS design which utilizes a line-interactive topology as defined as a Topaz isolation transformer, two Solar Electronics 8012-50-R-24-BNC LISNs (with line impedance stabilization networks), and an Avtron K490 load bank as a secondary power isolation unit for the protection of classified non-encrypted data processing for desktop/laptop computer solutions at DHS. This is a baseline for desktop/laptop workstation only, if power isolation is needed.

A separate CTTA approval is required for any equipment racks that support Top Secret or above installation under National Security Telecommunications and Information Systems Security Advisory Memorandum (NSTISSAM) TEMPEST 2-95A.

The APC Smart-UPS design will meet all requirements of Director of Central Intelligence Directives (DCID) 6/9 and Intelligence Community guidance under the provisions of DHS Management Directive, 11043, Sensitive Compartmented Information Program Management and NSTISSAM TEMPEST 2-95A "Amendment to Advisory Memorandum RED/BLACK Installation Guidance".

TEMPEST FILTERING

TEMPEST filtering shall be done IAW applicable security documents. Reference NSTISSAM TEMPEST/2-95, Red/Black Installation Guidance and contact SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD) for additional guidance.

HVAC COMPUTER EQUIPMENT ROOM (CER) REQUIREMENTS

HVAC AIR CONDITIONING

The CER requires cooled and filtered air. The air supply shall be a 24-hour/day 7-day/week system and be separately zoned and controlled from within the CER. Air filtering shall meet commercial codes.

TEMPERATURE ADJUSTMENTS

The room air supply shall be adjustable and provide a nominal return air temperature range between 64° and 75° Fahrenheit with all communications equipment installed and operational. National Security Agency standard.

HUMIDITY RANGE

Air supply humidity range shall be maintainable between 30 and 60 percent.

AIR SUPPLY DISSIPATION

The supply design shall be capable of dissipating a specified BTU/hr figure that meets the installed communications equipment wattage and humidity air input requirements. CIO project manager shall be responsible for ensuring the air dissipation specifications to provide to the site facilities personnel. Heat Dissipation guidelines are 750 to 5,000 BTUs per hour per cabinet. The following formula will be used to determine BTUs generated by installed equipment:

$(\text{Watts}) \times (.05689) \times (60 \text{ Hz}) = \text{BTUs per Hour}$

(Watts): Total watts consumed by installed communications equipment in a CER.

AIR HANDLER LOCATION

Coordination with the OCAO must be made prior to the installation of any type of air handling unit. OCAO also requires information regarding any planned air duct installations or preexisting infrastructure alterations. This will negate any interference with the CER design and installation. The location of the air handler should be in such a fashion to limit the amount of overhead obstructions. It is recommended a stand-alone wall unit be considered. The customer may contact the heating/air conditioning vendor of their choice for price and installation guidelines.

COMMUNICATION LINE INSTALLATION

Communication lines shall be installed in an approved conveyance; they shall not be installed loosely in ceilings, loosely installed under floors, or installed under carpeting.

CONVEYANCE SYSTEMS INSTALLED IN CEILINGS

Conveyance systems installed in the ceiling shall be no greater than 12 feet from the finished floor.

RED CONVEYANCE SYSTEMS UTILIZING WIRE

ACCESSIBILITY

All RED main backbone grid conveyance systems shall be accessible; therefore they shall not be installed within walls. This requirement does not apply for RED drop conveyances extending off the main backbone grid to individual stations (i.e., phones, PCs, etc.). Special security requirements may exist where a common wall is shared with uncleared individuals. Contact SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD) for guidance.

CONVEYANCE BENDS

All conveyance bends shall meet EIA / TIA standards.

CONVEYANCE SYSTEMS BETWEEN SCIFS

Conveyance systems between SCIFs that transit non-SCIF areas will require the approval of SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD). Media shall reside within a Protected Distribution System (PDS) or utilize Type 1 encryption. Contact SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD) for guidance.

PROTECTED DISTRIBUTION SYSTEM(S) (PDS)

PDS are used to transmit unencrypted classified NSI through an area of lesser classification or control. If the classified NSI is unencrypted, the PDS must provide adequate electrical, electromagnetic, and physical safeguards to deter exploitation.

Since PDS can be penetrated, given the opportunity and adequate time, a philosophy of detection of attempted penetration shall be employed. Careful consideration is given to the application before PDS is selected in preference to another INFOSEC system.

There may be economic, technical, or operational factors making PDS necessary in comparison to other INFOSEC systems. Although proper design and installation of PDS are important, continued physical security integrity after installation is critical. The cost and operational impact of maintaining the security of the system should be assessed prior to acquisition and installation, since such costs can easily exceed the installation cost.

Reference the National Security Telecommunications and Information Systems Security (NSTISSI) No.7003, 13 December 1996, PROTECTIVE DISTRIBUTION SYSTEMS (PDS) for detailed guidance on use of PDS.

All PDS must be approved in writing by the DHS Certified Technical TEMPEST Authority (CTTA).

PROTECTED DISTRIBUTION SYSTEMS (PDS) APPROVAL REQUEST

Requests for PDS approval shall be completed by the responsible SSO and forwarded to the department or agency Approval Authority, DHS Special Programs Security Division. It shall include the following information in each listed category:

1. Installation Site (Identify the organization where the PDS will be installed and a point-of-contact's name and phone number);
2. Installation Activity (Identify the organization responsible for the installation of the PDS, and a point-of-contact's name and phone number);
3. System Information (Provide a description of the components directly connecting to the PDS, and a summary of the type of cable used in the PDS (e.g., fiber optics, shielded twisted pair, coaxial cable) and the electrical parameters (e.g., voltage and current levels);
4. Security Profile (Identify the highest classification of NSI processed on the PDS (if special category information, identify the specific categories or compartments processed); and provide a percentage breakdown of the type of NSI processed on the PDS);
5. Facility Security (This section provides information concerning the security conditions of the facility where the PDS will be located by providing the following);
 - a. Indicate on a map of the residential and commercial area, the facility's approximate location;
 - b. Indicate a fenced facility's fence location on the map and describe the type of fencing construction (also, indicate if a perimeter Intrusion Detection System (IDS) is installed);
 - c. Indicate the automobile, pedestrian, and amphibious access points on the map;
 - d. Are guards posted at these access points, and what hours are the access points open;
 - e. Is a personnel badge recognition system used; are access lists maintained; and is an escort required for uncleared personnel;
 - f. Is a registration control system used for vehicles, employees, visitors, and tradesmen;
6. Building Security (This section requests information on security conditions of the building(s) within which the PDS will be installed as follows);
 - a. Provide a floor plan of the building(s), describe the exterior and interior construction, and identify whether or not the building's perimeter has an IDS installed;

- b. Indicate on the floor plan the access points to the building(s) (all windows accessible from the ground, fire escapes, etc. should be identified and any implemented window tamper protection devices should be described);
 - c. Are guards posted at the building access points, what hours are the access points open, and are cipher/simplex locks used for administrative access control to the building;
 - d. Indicate what type of doors and locks secure the access points;
 - e. Is a personnel badge recognition systems in use and are access lists maintained;
 - f. Indicate the clearance level of personnel entering the building, and if a clearance is required for unescorted access to the building;
 - g. Specify how the movement and operation of custodial, maintenance, and vending personnel is controlled, and if this requires an escort or continuous surveillance for uncleared personnel;
7. Protected Distribution Systems (PDS) (This section describes the security condition of PDS by providing the following information);
- a. Provide classification level of the area controlled, and indicate if uncleared personnel are monitored?
 - b. Indicate on a map or floor plan the location and routing of the proposed PDS. Describe its construction;
 - c. Describe the inspection procedures for detection of tampering; and
 - d. Will the PDS be alarmed, if so, describe in detail.

CONNECTIVITY GUIDELINES / GENERAL SPECIFICATIONS

COMMERCIAL DEMARCATION

Adequate space to meet installation requirements for common carrier interface / demarcation equipment shall be provided. The customer site is responsible for extending incoming Telco service from the Commercial Demarcation point to CER; a termination point (i.e. RJ-48) will be provided within the CER, which now becomes OCIO's service demarcation point. This includes installation of required conduit and cabling, terminating and cross connecting cabling at both ends and testing and labeling termination within CER.

During initial site survey, media and cable specifications will be determined. Generally this shall be copper cabling, either individually shielded pairs or two individually jacketed cables, segregating Transmit and Receive signals from Telco. The number of pairs installed to be dictated by site requirements. The CIO project manager shall determine specific location of the commercial service termination point within the CER

WIDE AREA NETWORK(S) (WAN) CONNECTIVITY

The customer is responsible for installing cable, connecting their infrastructure, to the GFE router. They must enter the cabinet via the existing conveyance and this cabling will be laced inside the cabinet using current installation practices, under the supervision of a COMM Maintenance technician. If the customer has chosen to install a fiber infrastructure they will be responsible for providing the conversion device (transceiver) for converting the signal from copper to fiber.

SECURE VIDEO TELECONFERENCING

Installation of video infrastructure shall employ the same type of media as the data infrastructure. The current network standard video equipment employs Video over IP technology and will use RJ45 connectors from the designated video wall plate to the video component. Cat 5 or higher UTP cabling will meet the video needs, however UTP may only be utilized if placed within Red conveyance devoid of any Black cabling; STP cabling is required if previously annotated requirement is unobtainable. If the site employs a fiber distribution system, fiber optic modems designed for fiber infrastructure & video will be utilized.

All commercially procured equipment to support the Video Teleconferencing (VTC) network within a SCIF requires a technical security evaluation prior to its installation and use, as well as Program Security approval.

Whether the media type is copper or fiber, both require a dedicated, continuous run between the VTC location(s), i.e. conference room, back to the CER. An exception to this is when Video/IP is being utilized for VTC purposes; termination is usually accomplished at a switch within an IDF location. The CIO project manager shall determine specific location.

If the customer site will only be provided DHS SCI Wide Area Network connectivity then a special connection will be required from the DHS SCI Wide Area Network router to the video components, bypassing the customers DHS SCI Wide Area Network firewall.

Wall plates will be marked as red or black and ideally, different type connectors should be used to prevent accidental connections.

NON-SECURE (BLACK) WALL PLATES (VOICE AND DATA)

The customer shall install, terminate and label all Black outlet/wall plates. All cables will be labeled at both ends. Wall plates shall be of a modular dual RJ-45 (digital data or voice) or RJ-11 (analog voice) jack types as appropriate. Labels on all cables shall indicate room and jack location for user end of the cable. The COMM preferred approach to infrastructure cabling is to utilize Cat 5 Shielded Twisted Pair (STP) copper wire for all voice cabling; CIO project manager shall specify specific cabling and pin-out (i.e. EIA-T568A or T568B) requirements. Station drops to extend from user office to MDF not located in CER. Terminate at MDF onto 110 blocks. Clearly label all drops at both user office and MDF.

NON-SECURE VOICE CABLE DISTRIBUTION

The design and installation of the unclassified (black) voice system in the SCIF must comply with Annex G, DCID 6/9 requirements. The exception to this would be if the customer were a government organization occupying government owned or leased space, in which case administrative (black) phone services may be provided by COMM. However, cable infrastructure installation shall remain the customer's responsibility. Program Security in conjunction with resolution of potential physical and technical security concerns must approve any administrative telephone system speakerphone capability, on a case-by-case basis. COMM requires an administrative phone be installed within close proximity to CER equipment to facilitate possible maintenance coordination activities. Contact SPECIAL SECURITY PROGRAMS DIVISIONS (SSPD) for additional guidance regarding any limitations.

SECURE (RED) WALL PLATES (VOICE AND DATA)

The customer shall install, terminate and label all data outlet/wall plates. All cables will be labeled at both ends. The COMM preferred approach to infrastructure cabling is to utilize Cat 5 Shielded Twisted Pair (STP) copper wire for all voice cabling; CIO project manager shall specify specific cable and pin-out (i.e. EIA-T568A or T568B) requirements.

If media type is Multimode (MM) fiber, wall plates shall be terminated in accordance with pre-established facility standards. All cables will be properly identified at both termination ends.

SECURE VOICE CABLE DISTRIBUTION (TDM)

The cables shall be terminated and labeled at a termination block (i.e. 66/110) at the CER end, and CIO project manager shall specify specific cable and pin-out (i.e. EIA-T568A or T568B) requirements at office drop end.

SECURE VOICE CABLE DISTRIBUTION (IP)

Secure Voice cables shall be terminated at a termination block (i.e. 66/110) at the CER end, and CIO project manager shall specify specific cable and pin-out (i.e. EIA-T568A or T568B) requirements. CIO project manager may tailor as appropriate to facilitate specific installation requirements.

INFRASTRUCTURE CABLING

The COMM preferred approach to infrastructure cabling is to utilize Cat 5 Shielded Twisted Pair (STP) copper wire for all secure data and voice cabling. This type of infrastructure is more cost effective than fiber for the cabling, installation and the cost of associated switching equipment.

For larger installations with multiple TC/IDF closets, COMM recommends using multi-mode fiber optic cable be run from the CER to the TC/IDF, with Cat 5 STP copper extending out from the TC/IDF to the wall plate. In this case fiber optics must be terminated to a fiber optic patch panel within TC/IDF.

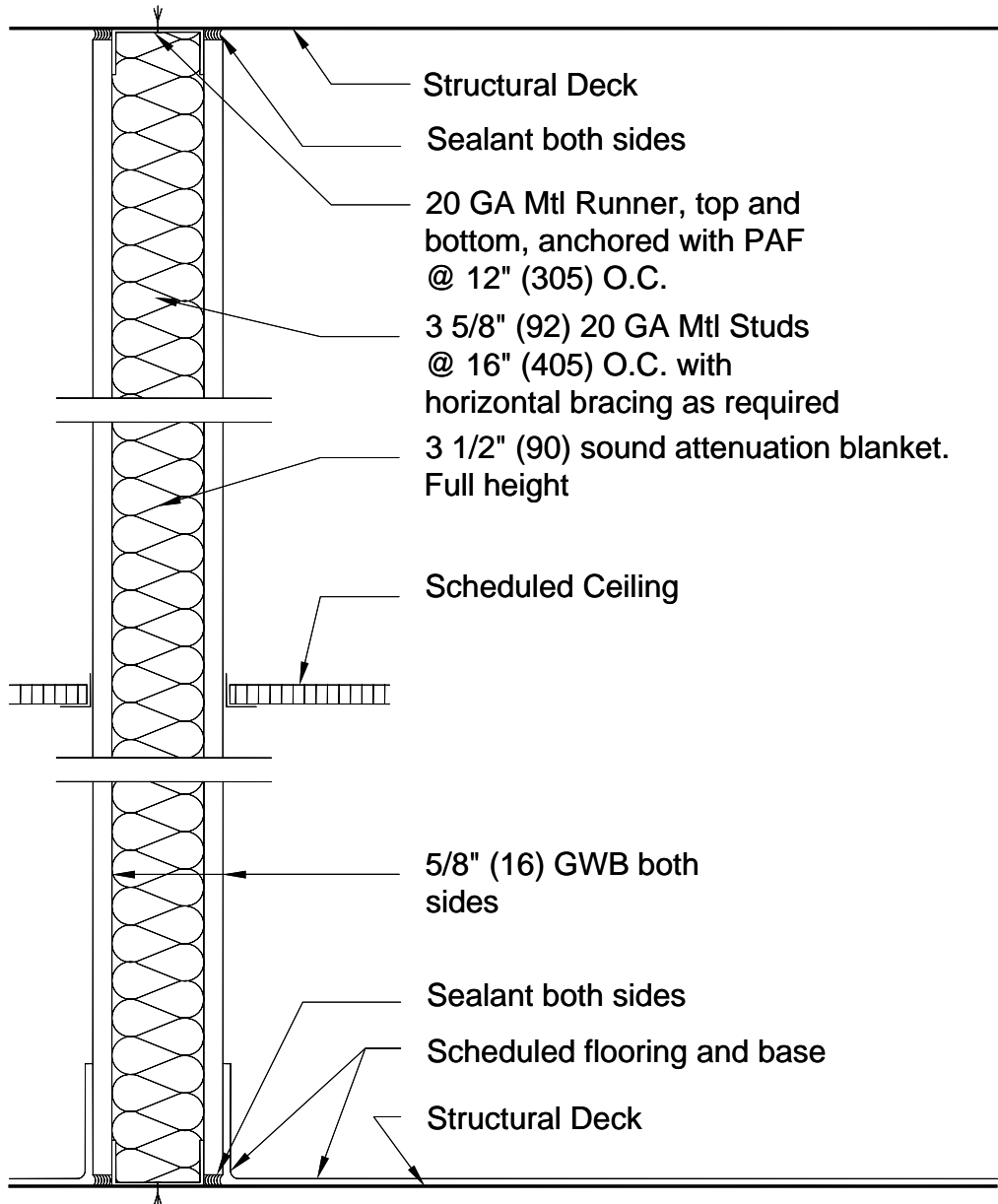
STP cabling, which supports secure voice (TDM only) connectivity, will be terminated at a 110 punch down block within CER and any TC/IDF as it transverses between the customer's wall plate and CER location. These connections shall be labeled and tested by the installer.

STP cabling, which supports secure data connectivity will be terminated per CIO project manager's direction. COMM recommends utilization of patch panels for versatility, and for addressing any varying security levels that may require isolation. Regarding data connections, cables will be terminated at a patch panel.

STANDARD WALL DESIGNS / DUCT DETAILS / FIGURES

**** Every element of SCIF perimeter wall(s) installation must be made available for inspection by the government representative prior to concealment. ****

WALL TYPE 1 - ACOUSTICALLY-TREATED PARTITION
 (NOT A SCIF PERIMETER PARTITION)

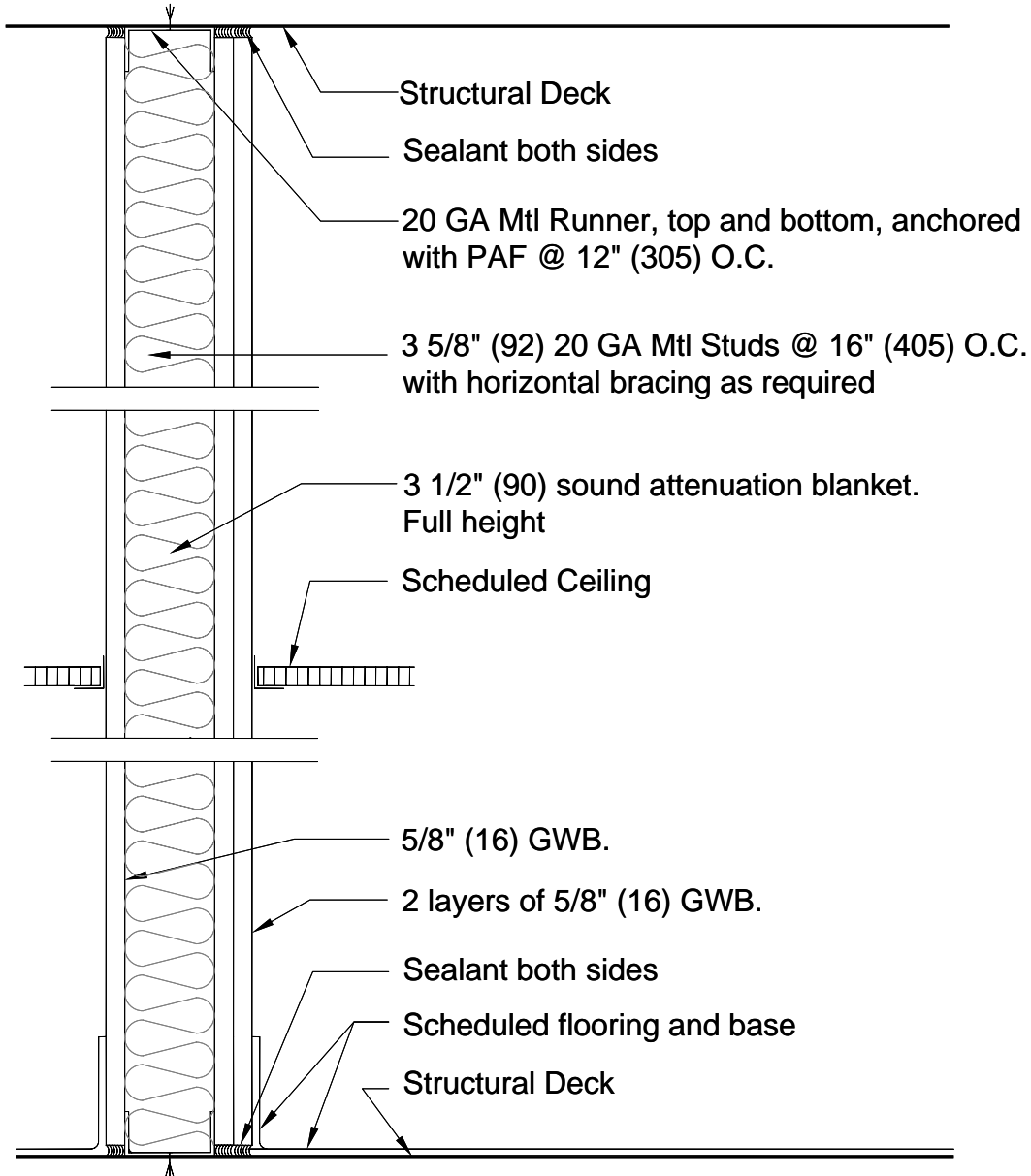


Rev. 02-01-07

Wall Type 1 (Acoustic Wall)

(NOT A SCIF PERIMETER PARTITION)

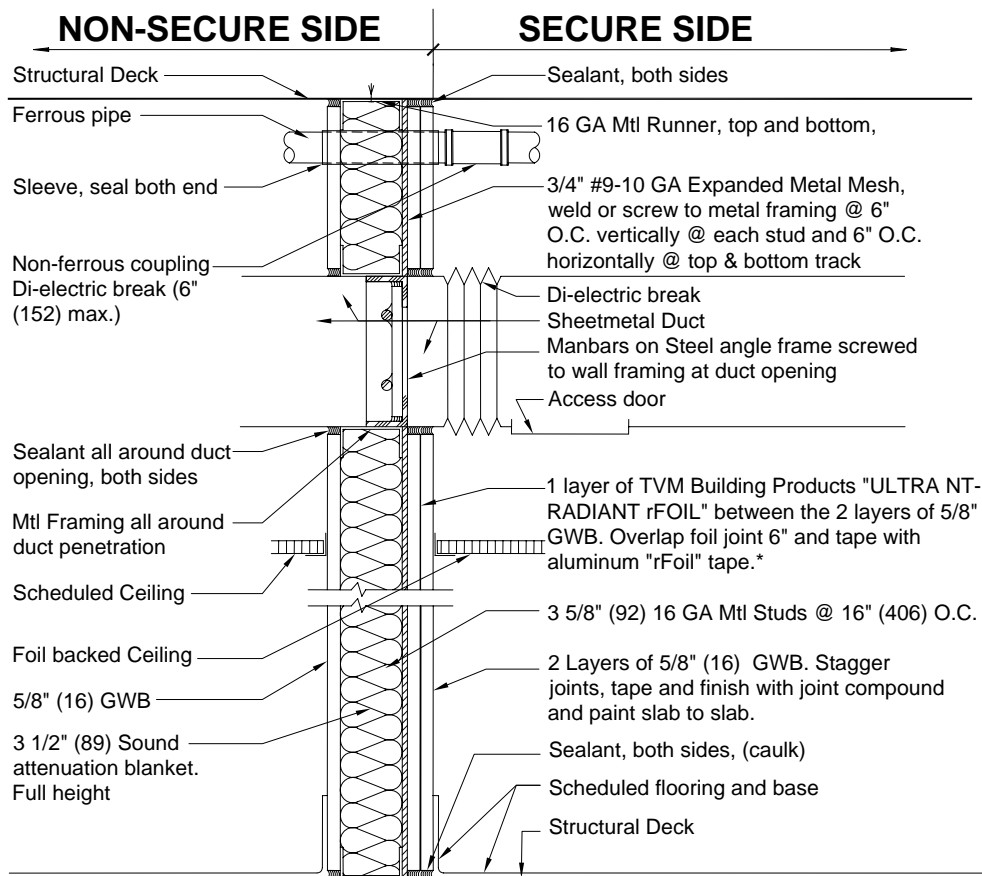
WALL TYPE 2: - ACOUSTICALLY-TREATED PARTITION (STC-45)
 (NOT A SCIF PERIMETER PARTITION)



Rev. 02-01-07

Wall Type 2 (STC 45)
 (Compartment and Closed Storage Wall)

WALL TYPE 3A: - SCIF WALL PERIMETER WALL PARTITION



Wall Type 3A (SCIF PERIMETER WALL PARTITION)

Rev. 02-01-07

Conduit/pipe penetrations through wall type A6a shall be sealed all around, and shall be fitted with a dielectric break within 6" (152) of the wall at the secure side of the room.

Duct penetrations on the wall type 3A shall be sealed all around, and shall be fitted with a dielectric break within 6" (152) at the secure room side of the wall. A 12"X12" (305x305) access panel shall be provided in the bottom of the duct. Duct openings larger than 96 SqIn (61,935) (unless one dimension is 6" (152) or less) shall be protected with 1/2" (13) manbars spaced and welded at 6" (152) O.C. horizontally and vertically - refer manbar detail.

"ULTRA NT- RADIANT rFOIL" shall be used between the 2 layers of 5/8" GWB. Overlap foil joint 6" and tape with aluminum "rFoil" tape, or approved equivalent product

* 2 layers of 5/8" aluminum foil backed GWB may be used in lieu of "ULTRA NT- RADIANT rFOIL". First layer of GWB joints shall be taped with "rFoil" tape. Joints of second layer shall be offset staggered from joints in first layer.

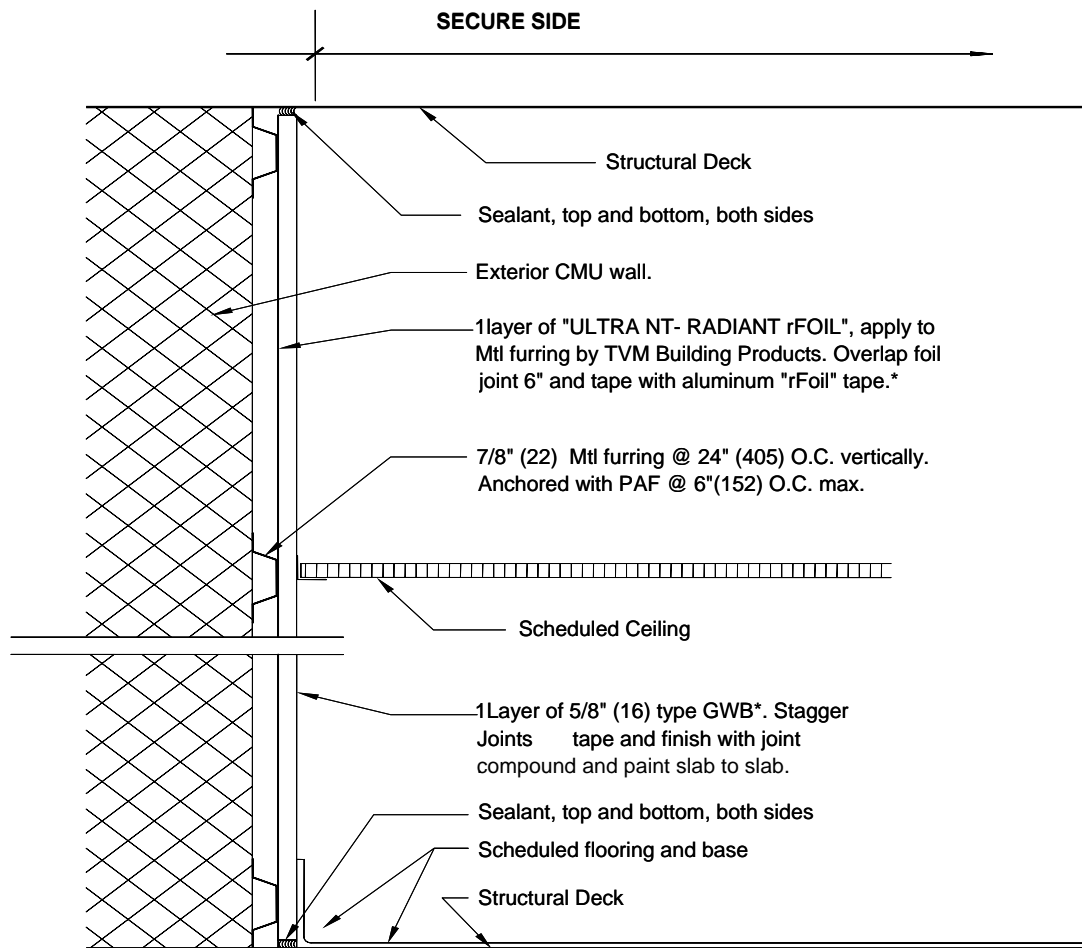
Partition shall be sealed continuously with an acoustical sealant wherever it abuts another element (i.e. wall, column, mullion, etc.) Gypsum board joints shall be taped and finished with joint compound slab to slab.

Expanded Carbon Steel Security Mesh to be ASTM A569/569M, ASTM F1267, Type II, Class1, standard, flattened, style 3/4" #9-10 GA, 171 lbs/csf. SWD=.923" (23), LWD=2.1"(53) with overall thickness of 0.120 with max. open area of 63%. Metal mesh to be welded or screwed to metal framing at 6" (150) O.C. at each stud and horizontally at top and bottom track. If screws are used as the method of attachment 1" diameter shall be used with each screw.

If wall abuts adjoining tenant, all electrical wiring and boxes shall be surface mounted on the secure side.

FOR OFFICIAL USE ONLY

WALL TYPE 3B - SCIF WALL PARTITION ON PERIMETER WALL



Rev. 02-01-07

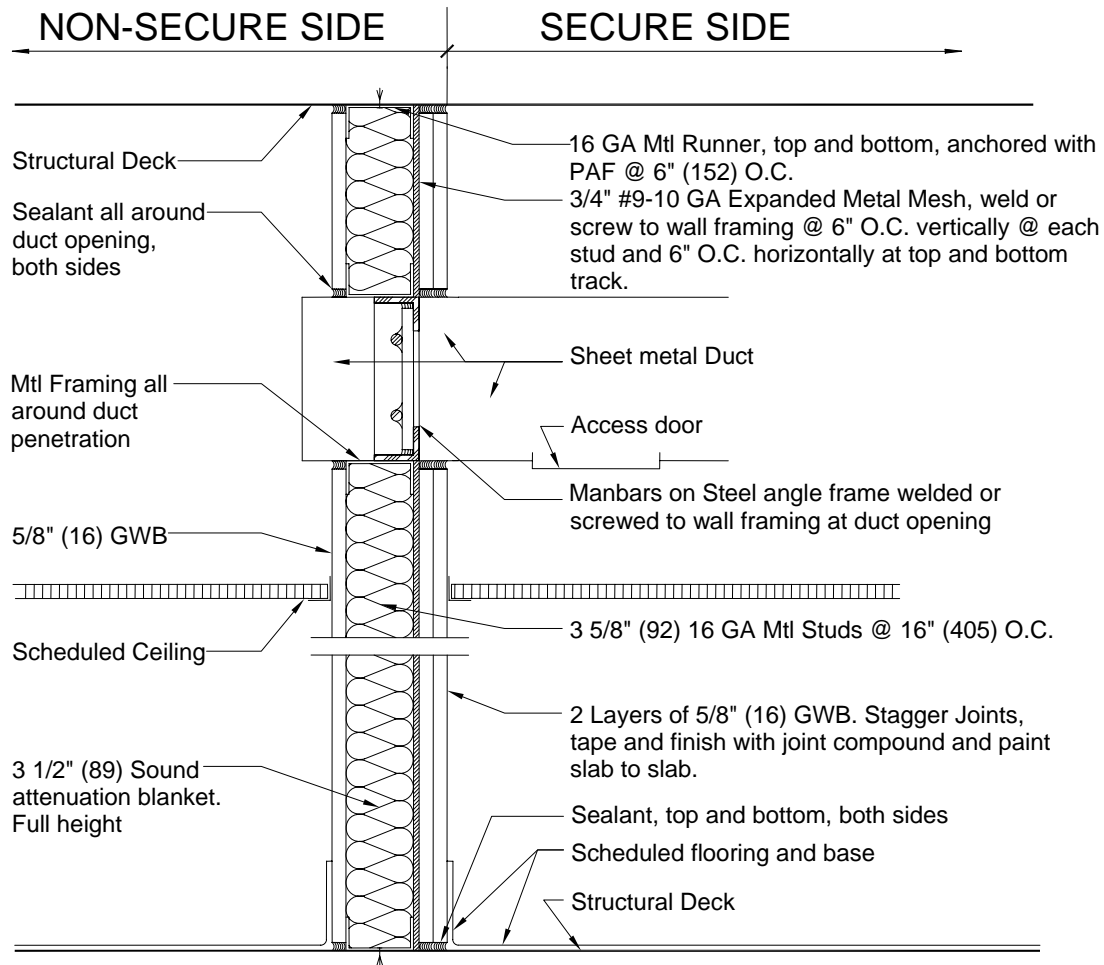
Wall Type 3B (Building Perimeter SCIF Wall)

Conduit /pipe penetrations through wall type 3B shall be sealed all around. Partition shall be sealed continuously with a sealant wherever it abuts another element (i.e. wall, column, mullion, etc.) A double layer of RF foil (example product TVM ultra Radiant NT Foil) or similar approved product. Overlap foil joint 6" and tape with aluminum "rFoil" tape.

** 2 layers of 5/8" 2 layers of 5/8" aluminum foil backed GWB may be used in lieu of "ULTRA NT- RADIANT rFOIL". First layer of GWB joints shall be taped with "rFoil" tape. Joints of second layer shall be offset staggered from joints in first layer.

**** Every element of SCIF perimeter wall(s) installation must be made available for inspection by the government representative prior to concealment. ****

WALL TYPE 4 - SECURE PERIMETER PARTITION
 (NON-SCIF PERIMETER PARTITION)



Rev. 02-01-07

Wall Type 4 (Collateral Area Perimeter Wall, STC-45)

Conduit/pipe penetrations through wall type 4 shall be sealed all around.

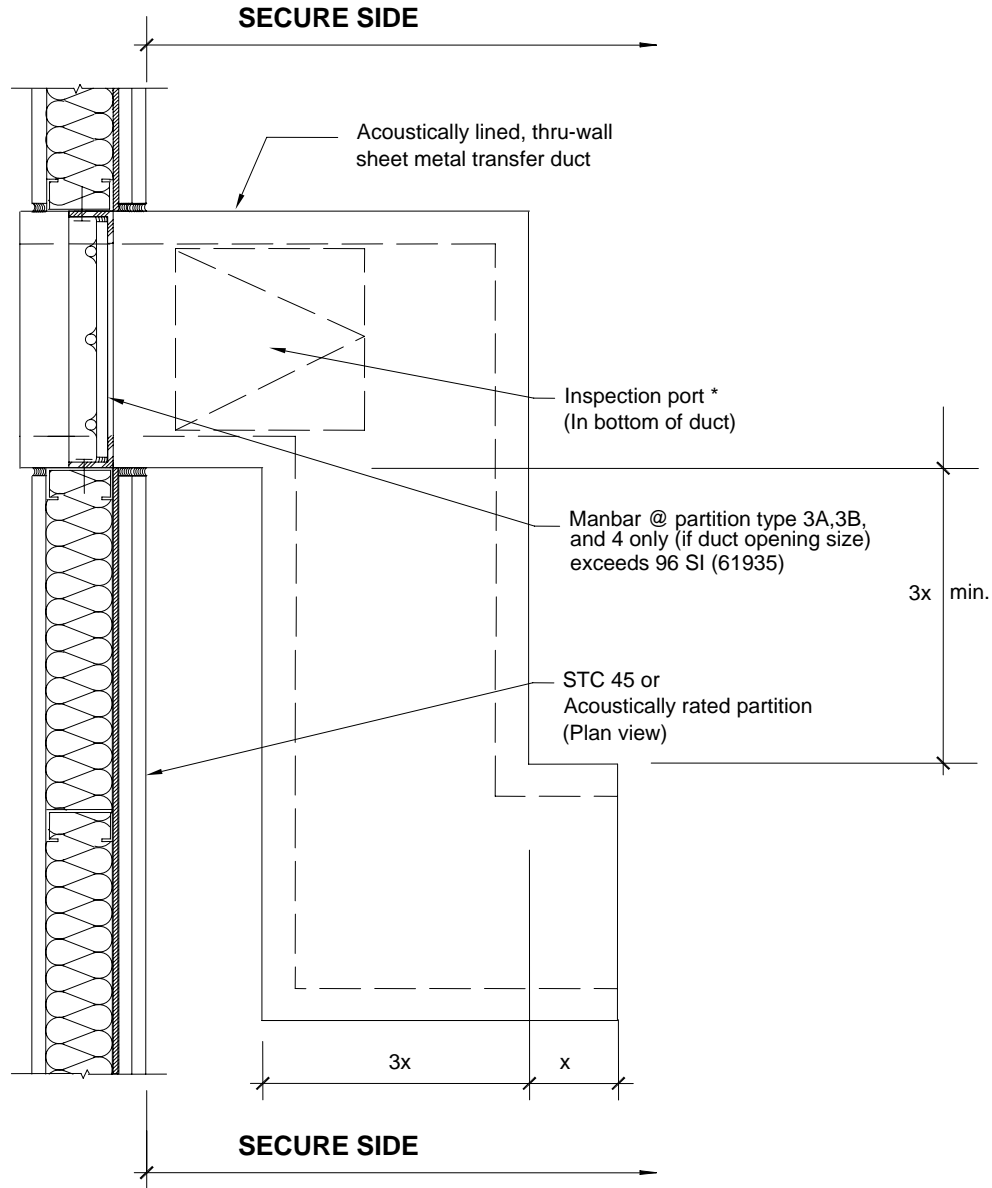
Duct penetrations through wall type 4 shall be sealed all around, and shall be fitted with a 12"X12" (305x305) access panel in the bottom of the duct on the Secure Side. Duct openings larger than 96 Sq in (61,935) (unless one dimension is 6" (152) or less) shall be protected with 1/2" (13) manbars spaced and welded at 6" (152) O.C. horizontally and vertically - refer to manbar detail.

Partition shall be sealed continuously with a sealant wherever it abuts another element (i.e. wall, column, mullion, etc.)

Expanded Carbon Steel Security Mesh to be ASTM A569/569M, ASTM F1267, Type II, Class 1, standard, flattened, style 3/4" #9-10 GA, 171 lbs/csf. SWD=.923" (23), LWD=2.1"(53) with overall thickness of 0.120 with max. open area of 63%. Metal mesh to be welded or screwed to metal framing at 6" (152) O.C. at each stud and 6" O.C. horizontally @ top & bottom track. If screws are used as the method of attachment 1" diameter washer shall be used with each screw.

If wall abuts adjoining tenant, all electrical wiring and boxes shall be surface mounted on the secure side.

TRANSFER DUCT -Z-DUCT / PASSIVE AIR RETURN



Note: Return air grilles shall be min. 25'-0" (7620) from 'Z' duct opening

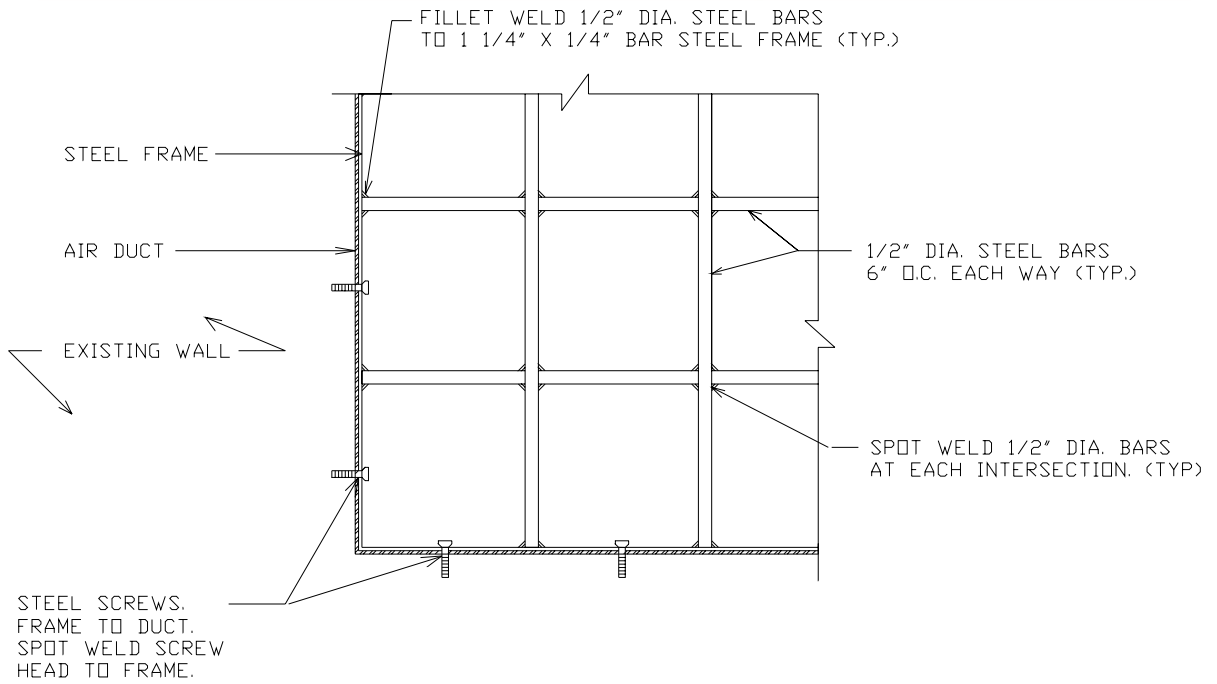
Duct Penetration (Plan View)

Rev. 02-01-2007

If the Z-Duct cannot be placed on the secure side of the facility it can be placed on the exterior of the SCIF but must be inspectible. A high security hasp and pad lock must be installed on the inspection port if located on the exterior of the SCIF.

*** Inspection port(s) shall allow space for visual and physical inspection of man-bar installation.**

MANBAR BARRIER

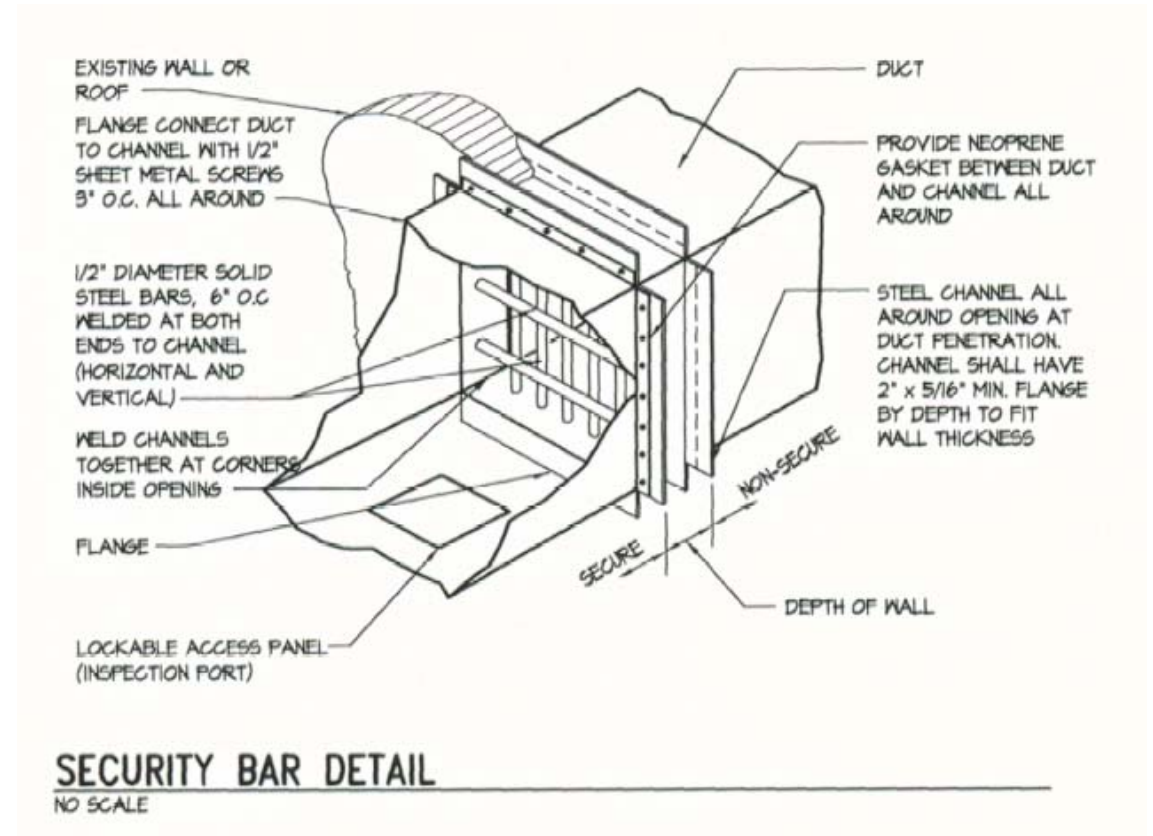
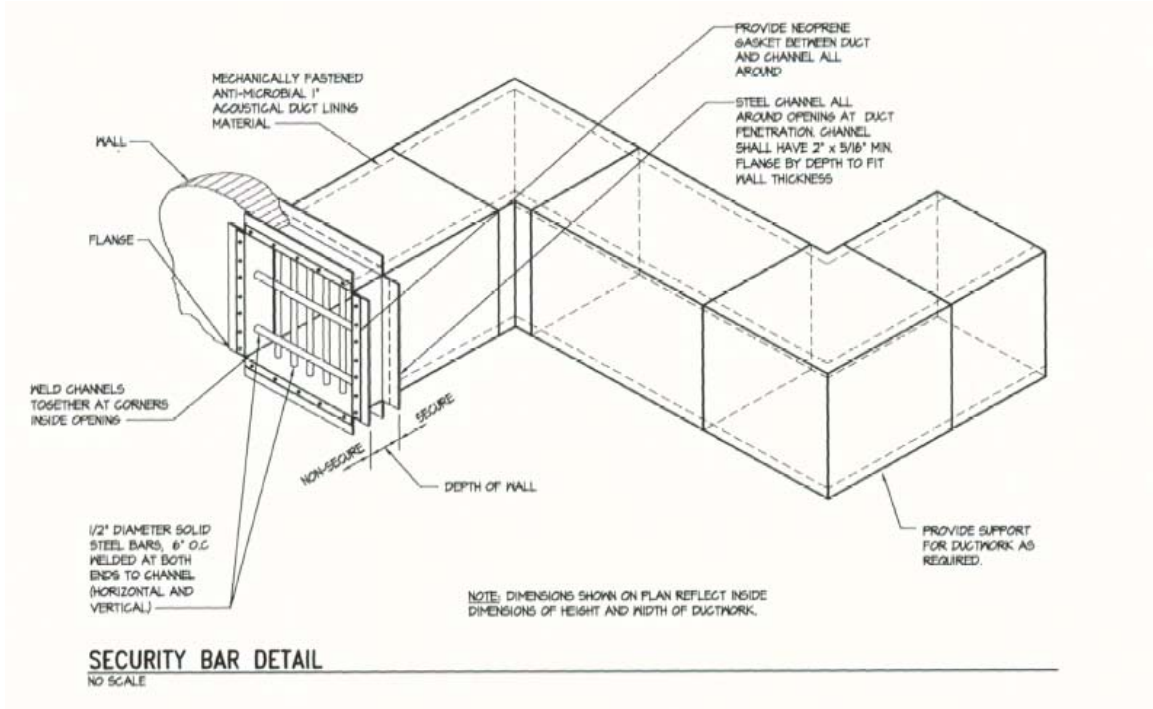


NOTE:
 MANBARS SHALL BE REQUIRED FOR ANY PENETRATION LARGER THAN 96 SQ.IN OF ANY PERIMETER WALLS, GUN VAULTS, AND EVIDENCE ROOMS.

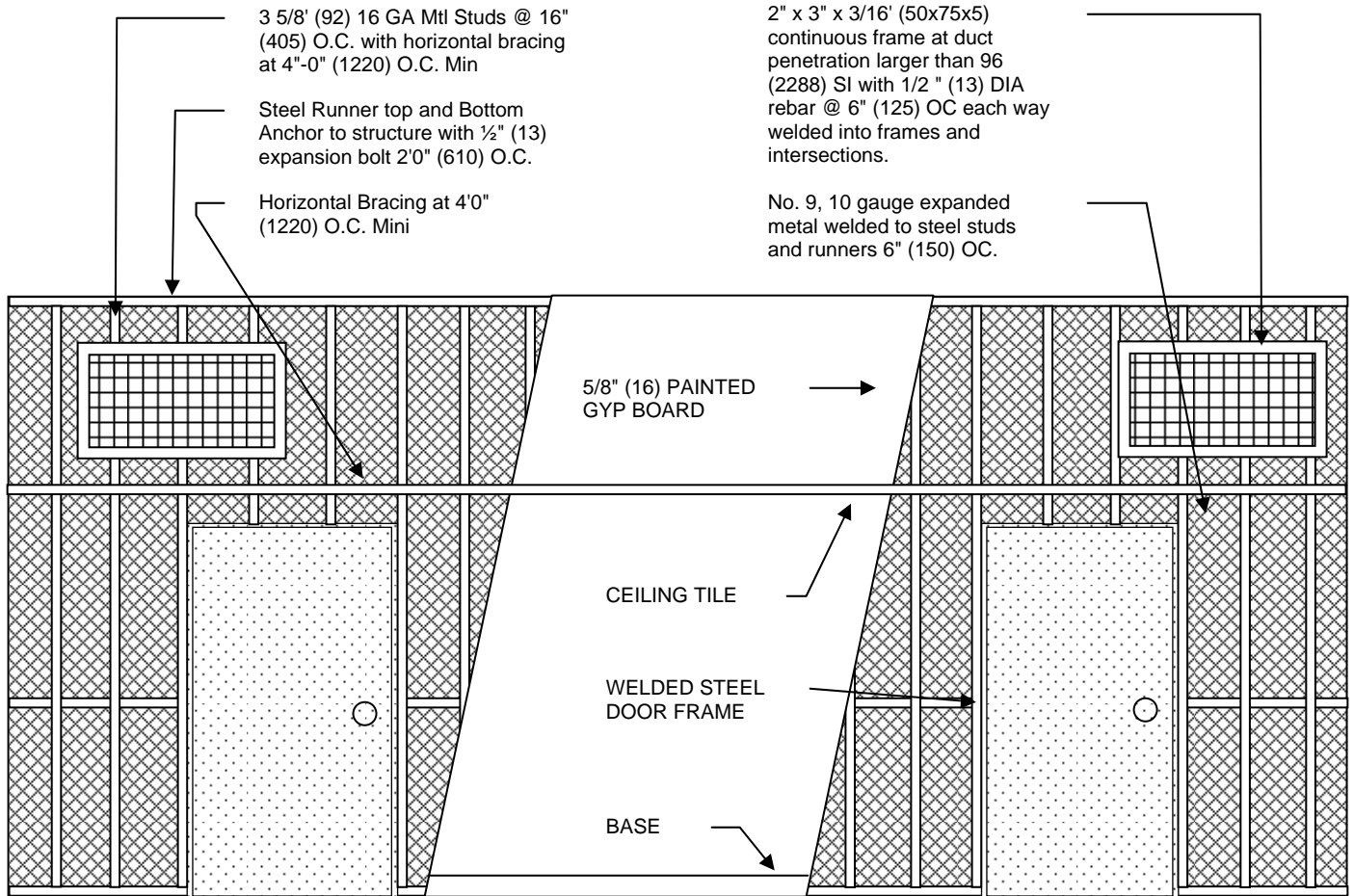
NOT TO SCALE
 REV: 02-01-2007

WALL D: MANBAR BARRIER

SECURITY BAR DETAIL

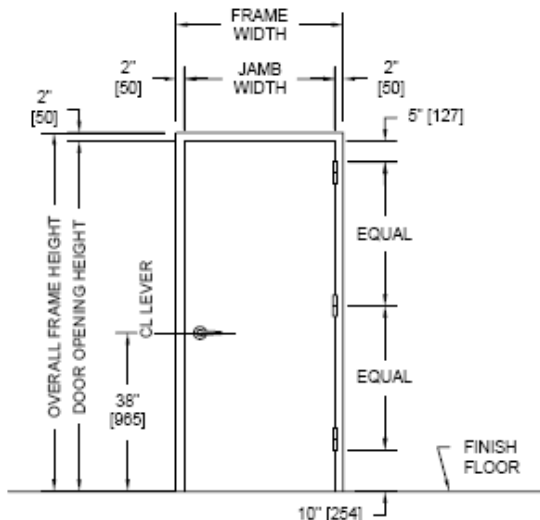


SECURITY GRILL/PERIMETER WALL ELEVATION DETAIL



NOT TO SCALE
REV: 02-01-2007

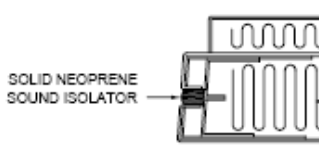
SAMPLE - UL FIRE RATED / STC RATED / DOOR AND FRAME ASSEMBLY



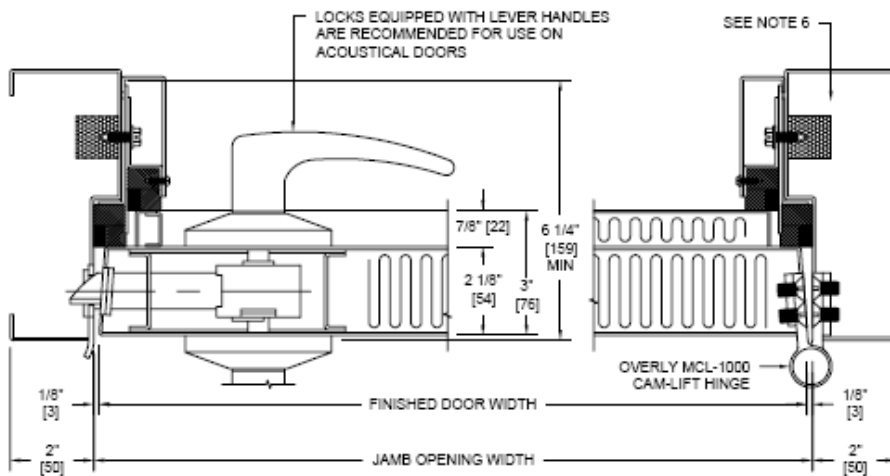
PUBLIC SIDE ELEVATION
RIGHT HAND REVERSE BEVEL SHOWN

NOTES:

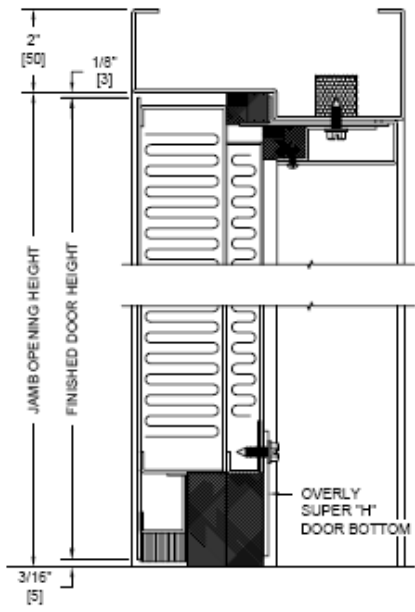
1. All exposed surfaces of door and frame to receive one coat of rust inhibitive prime paint.
2. Door bottom requires flush level sealing surface. Wood, aluminum, or stainless steel threshold recommended. Do not seal against carpet.
3. Frame is equipped with Overly dual compression seals at head and jambs. Door is equipped with an Overly Super "H" door bottom.
4. Door weight is 20.4 pounds per square foot.
5. Door can be equipped with standard builders hardware, Customer to specify. Concealed hardware is not recommended for acoustical doors.
6. Frames equipped with masonry anchors must be grouted full in field. Bolt-in type frames must have all voids in head and jambs packed with 8 to 12 pound density mineral wool and all voids between wall and frame continuously caulked.
7. UL fire labels available in compliance with UL10B and UL10C/UBC7-2. Consult factory for specifics.
8. Unit tested as single door at Riverbank Acoustical Laboratories. Results are described in Test Report No. TL92-175 with sound transmission results as shown in chart below.
9. The panel on the interior side of the door is factory recessed to accommodate cylindrical locksets. Mortise locksets require extension of push side cylinders, spindles, and thru-bolt screws.
10. Door construction is covered by US Patent No. 5,417,029.



TYPICAL EDGE CONSTRUCTION
ABOVE AND BELOW LOCK CUTOUTS



HORIZONTAL SECTION



VERTICAL SECTION

SOUND TRANSMISSION LOSS IN dB AT FREQUENCY / HERTZ																	
100	125	160	200	250	315	400	500	630	800	1000	1250	1600	2000	2500	3150	4000	5000
38	39	39	42	44	46	51	52	53	55	55	58	61	63	64	67	69	70

ALL DIMENSIONS BOTH IN INCHES AND MILLIMETERS

SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT (FIBERPLEX)

FOI-2170 AND FOI-2171



PRODUCT LINE:

Fiber Optic Isolator

CATEGORY:

Video

Uni-Directional (Simplex)
Composite Video

FOI-2170: Optical Transmitter

FOI-2171: Optical Receiver



FOI-2170-ST and FOI-2171-ST

FEATURES

- Video Bandwidth: 4 Hz to 7 MHz
- Compatible with:
 - NTSC
 - PAL
 - SECAM
- Compliant with:
 - EIA / RS-170
 - EIA / RS-170A
 - EIA / RS-330

DESCRIPTION

The FOI-2170 and FOI-2171 both provide complete electrical isolation for composite video communications. The units are compatible with NTSC, PAL, and SECAM video broadcast standards. The units are transparent to all monochrome RS-170, color RS170A, and closed circuit RS-330 video. The FOI-2171 has an AGC (automatic gain control) to stabilize the video output for different fiber optic cable lengths. Adjusting the AGC potentiometer will also increase or decrease the overall scene brightness.

The units can be used in areas of high electrical noise or in and out of RF shielded enclosures. The units enhance privacy of communications because fiber can not be tapped without being detected and does not radiate any emissions. The fiber optic cable is not susceptible to interference caused by impulse noise, crosstalk, or EMI. The potential problem of creating ground loops or ground offsets is also eliminated because there is no conductive path through the glass fiber for ground.

In addition, fiber optic cable offers much longer transmission distances than traditional coax cabling. Multimode optics on the units can extend the distance to 2km. A typical link consists of an FOI-2170 at one end of the network transmitting optical signals to an FOI-2171 at the other end of the network as shown under "TYPICAL APPLICATION".

FiberPlex, Inc.
10840-412 Guilford Rd

Annapolis Junction
Maryland 20701

Phone: 301-604-0100
Fax: 301-604-0773

www.fiberplex.com
sales@fiberplex.com

4/27/06
page 1 of 4

NOT TO SCALE
REV: 02-01-2007

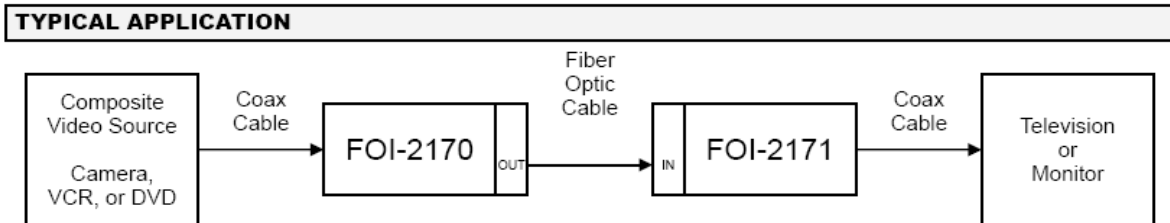
SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT

FOI-2170 AND FOI-2171



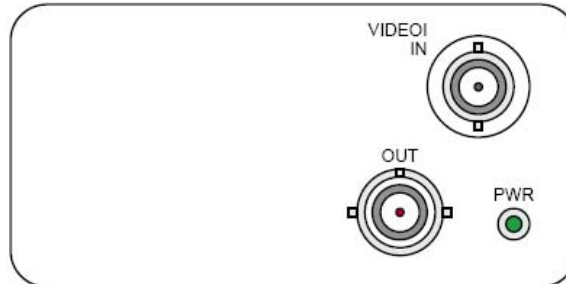
SPECIFICATIONS					
		minimum	typical	maximum	unit
Power Requirement	Voltage Range	7	9	12	V
	Supply Current	-	200	-	mA
Environmental	Storage Temperature	-40	-	85	°C
	Operating Temperature	0	-	50	°C
Video	Bandwidth (-3 dB)	4 Hz to 7 MHz			
	Signal to Noise Ratio (SNR)	45 dB unrated, 56 dB rated			
	AGC Range	10:1			
	Interface Connector	BNC			
Case Dimensions	Size 2	width	height	length	unit
		1.312	2.562	4.5	inches

OPTICAL CHARACTERISTICS						
Fiber	Size	Max Distance	Wavelength	FOI-2170 Output Power	FOI-2171 Receiver Sensitivity	Loss Budget
Multimode	62.5 / 125 μ m	2 km	820 nm	-18 dBm	-30 dBm	12 dB

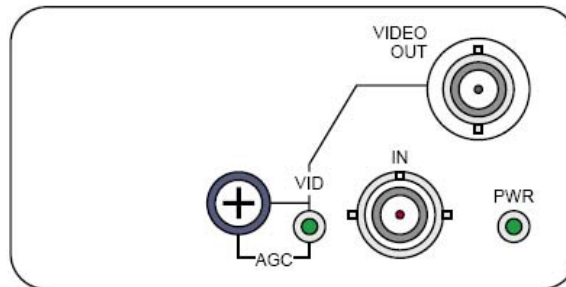


SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT

FOI-2170 AND FOI-2171



FOI-2170-ST Front View



FOI-2171-ST Front View

LED INDICATORS			
Model	Label	Color	Description
FOI-2170 and FOI-2171	PWR	Green	Power supply in FOI unit is operating properly.
		Off	No power from the PSQ power supply or open fuse inside the FOI unit. Check that the PSQ power supply is operating properly. If the PSQ power supply is good, separate the FOI unit from the PSQ power supply for 30 seconds and then reattach so that the fuse inside the FOI unit has time to reset. If the PWR led is still off or not constant, replace the FOI unit.
FOI-2171	VID	Green	The AGC (automatic gain control) has stabilized the VIDEO OUT voltage to the reference voltage set by the AGC potentiometer. The overall scene brightness will increase or decrease depending on the reference voltage.
		Off	The AGC (automatic gain control) is busy measuring the VIDEO OUT voltage and comparing it to the reference voltage set by the AGC potentiometer. Weak video signals will be amplified and strong video signals will be attenuated until the AGC loop stabilizes.

SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT

FOI-2170 AND FOI-2171

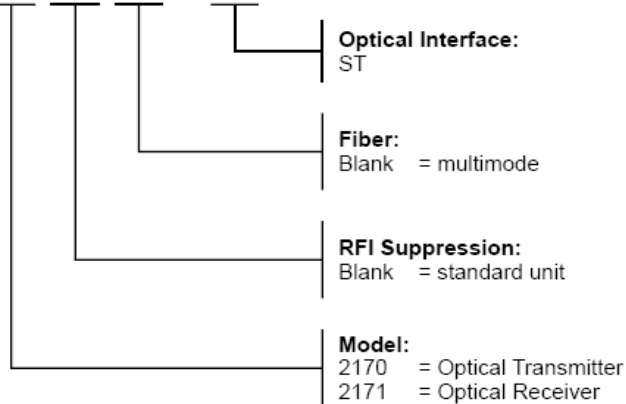


ACCESSORIES

Model	Description
CMA-2001	Chassis Mount Adapter for RMC-2101
CMA-3002	Chassis Mount Adapter for RMC-3101, RMC-3102, and RMC-3201
PSQ-2910	Power Supply for FOI-2xxx series
RMC-2101	Rack Mount Chassis, 3-1/2" H x 19" W, rear access
RMC-2101	Rack Mount Chassis, 3-1/2" H x 19" W, rear access with front exhaust fans
RMC-3101	Rack Mount Chassis, 5-1/4" H x 19" W, front access
RMC-3102	Rack Mount Chassis, 5-1/4" H x 19" W, front access with optical patch panel
RMC-3201	Rack Mount Chassis, 5-1/4" H x 19" W, rear access
RMC-4101	Rack Mount Chassis, 5-1/4" H x 19" W, front access with rear exhaust fans and perforated front panel
WMA-2001	Wall Mount Adapter with optical patch
WMA-3002	Wall Mount Adapter

ORDERING INFORMATION

FOI -



Available Options:

FOI-2170-ST
FOI-2171-ST

- For special applications that require custom units, please call FiberPlex for more information.

SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT (PCT-FTX3R)

FIBER OPTIC ACTIVES

1310 NM CATV TRANSMITTER



PCT's 1310 nm Rackmount Transmitter (PCT-FTX3R) is an industry standard rack-mounted CATV transmitter suitable for NTSC or PAL television signal transmission. Analog bandwidth to 870 MHz allows for advanced services such as HDTV, VOD, PPV, and high speed data as well as traditional cable TV.



FEATURES & BENEFITS

- 1U 19 in. rack housing
- High performance cooled DFB laser diode
- Patented linearization circuitry
- 870 MHz forward bandwidth
- Optical power range from 6 to 20 mW
- Link budget up to 14 dB with received power = -1 dBm
- AGC / MGC gain control mode
- LCD display and control
- LED status indicator lights

APPLICATIONS

- Narrowcast and broadcast applications for transmission of analog and digital video, data, and voice

ORDERING INFORMATION

PART NO.	DESCRIPTION
PCT-FTX3R-8AS	Fiber Optic Transmitter, 1310 nm, 8 dB Link Budget Based on -1 dBm, 6mW, SC/APC
PCT-FTX3R-10AS	Fiber Optic Transmitter, 1310 nm, 10 dB Link Budget Based on -1 dBm, 8mW, SC/APC
PCT-FTX3R-11AS	Fiber Optic Transmitter, 1310 nm, 11 dB Link Budget Based on -1 dBm, 10mW, SC/APC
PCT-FTX3R-12AS	Fiber Optic Transmitter, 1310 nm, 12 dB Link Budget Based on -1 dBm, 13mW, SC/APC
PCT-FTX3R-13AS	Fiber Optic Transmitter, 1310 nm, 13 dB Link Budget Based on -1 dBm, 16mW, SC/APC
PCT-FTX3R-14AS	Fiber Optic Transmitter, 1310 nm, 14 dB Link Budget Based on -1 dBm, 20mW, SC/APC

Other Connector Options:

US = SC/UPC; FS = FC/APC; FU = FC/UPC

SUGGESTED CABLE TELEVISION ISOLATION EQUIPMENT (PCT-FTX3R)



1310 NM CATV TRANSMITTER

FIBER OPTIC ACTIVES

SPECIFICATIONS

PCT-FTX3R

OPTICAL

Wavelength	1310 ± 20 nm
Connector	SC/APC; FC/APC
Output Power	6 to 20 mW

RF

Input Level	20 dBmV / channel ± 5 dB
Gain Control Range	10 dB
Input Impedance	75 Ω
Return Loss	> 16 dB
Connector Type	F - Female

LINK PERFORMANCE

CNR vs Link Loss	See table below
CSO	≤ -63 dBc
CTB	≤ -67 dBc
XMOD	≤ -65 dBc
Bandwidth	45 to 870 MHz
Flatness	±0.75 dB
Channel Loading	77 NTSC channels + 200 MHz digital channels

CNR VS LINK LOSS (Guarenteed Minimum Performance)

MODEL	OUTPUT POWER	6 dB	7 dB	8 dB	9 dB	10 dB	11 dB	12 dB	13 dB	14 dB
PCT-FTX3R-8	6 mW	53	52	51	50					
PCT-FTX3R-10	8 mW			53	52	51	50			
PCT-FTX3R-11	10 mW				53	52	51	50		
PCT-FTX3R-12	13 mW					53	52	51	50	
PCT-FTX3R-13	16 mW						53	52	51	50
PCT-FTX3R-14	20 mW							52	51	50

POWER REQUIREMENT

Standard	90 to 260 VAC, 50 / 60Hz
Power Consumption	15 W Max.

ENVIRONMENTAL

Operating Temperature Range	0 to 50° C (32 to 122° F)
Storage Temperature Range	-40 to 70° C (-4 to 158° F)
Relative Humidity	85% Max.

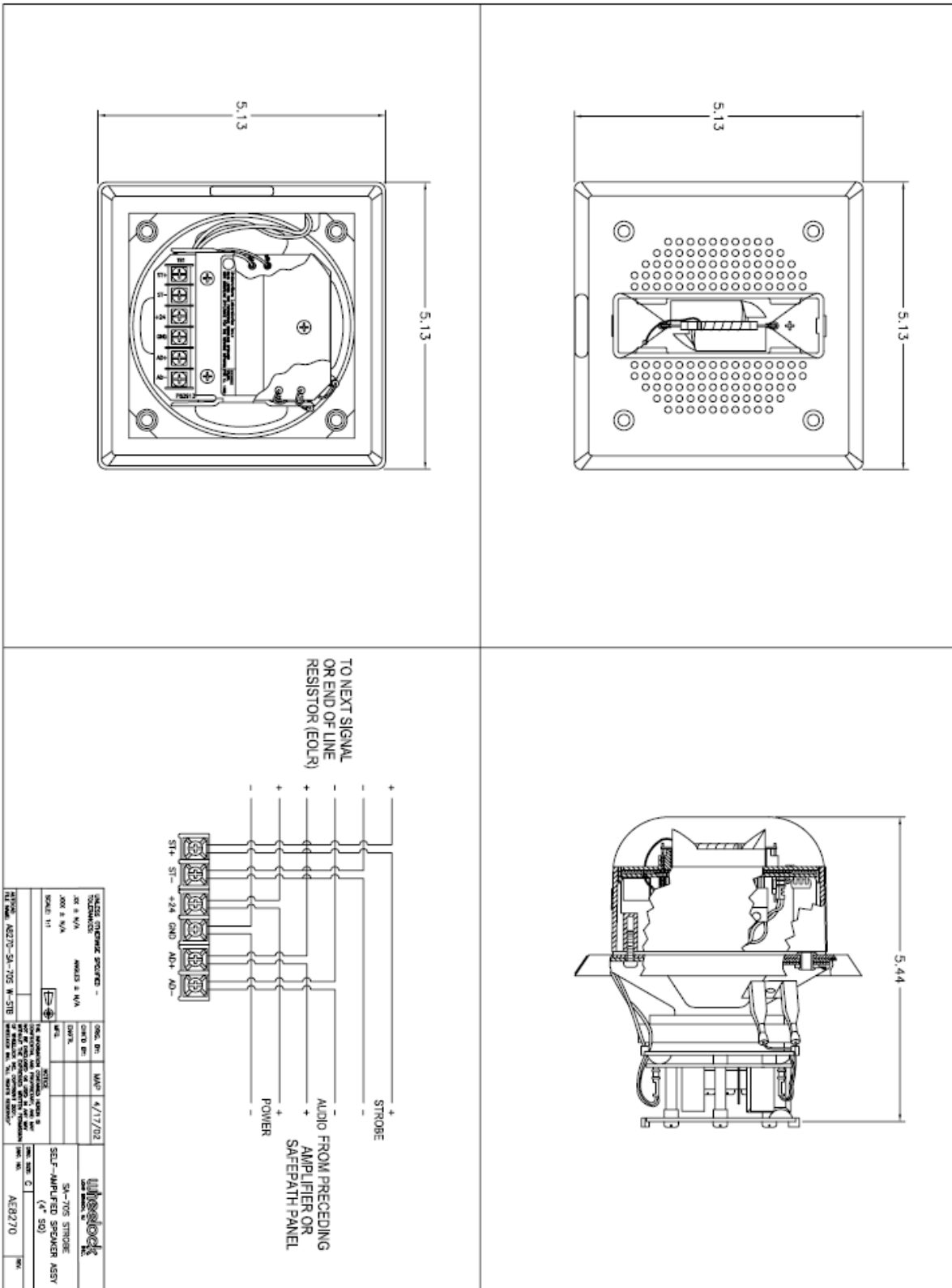
PHYSICAL PROPERTIES

Dimensions (W x D x H)	8.5 x 35 x 4.5 cm (3.3 x 13.8 x 1.8 in.)
Weight	4.5 kg (9.9 lbs.)

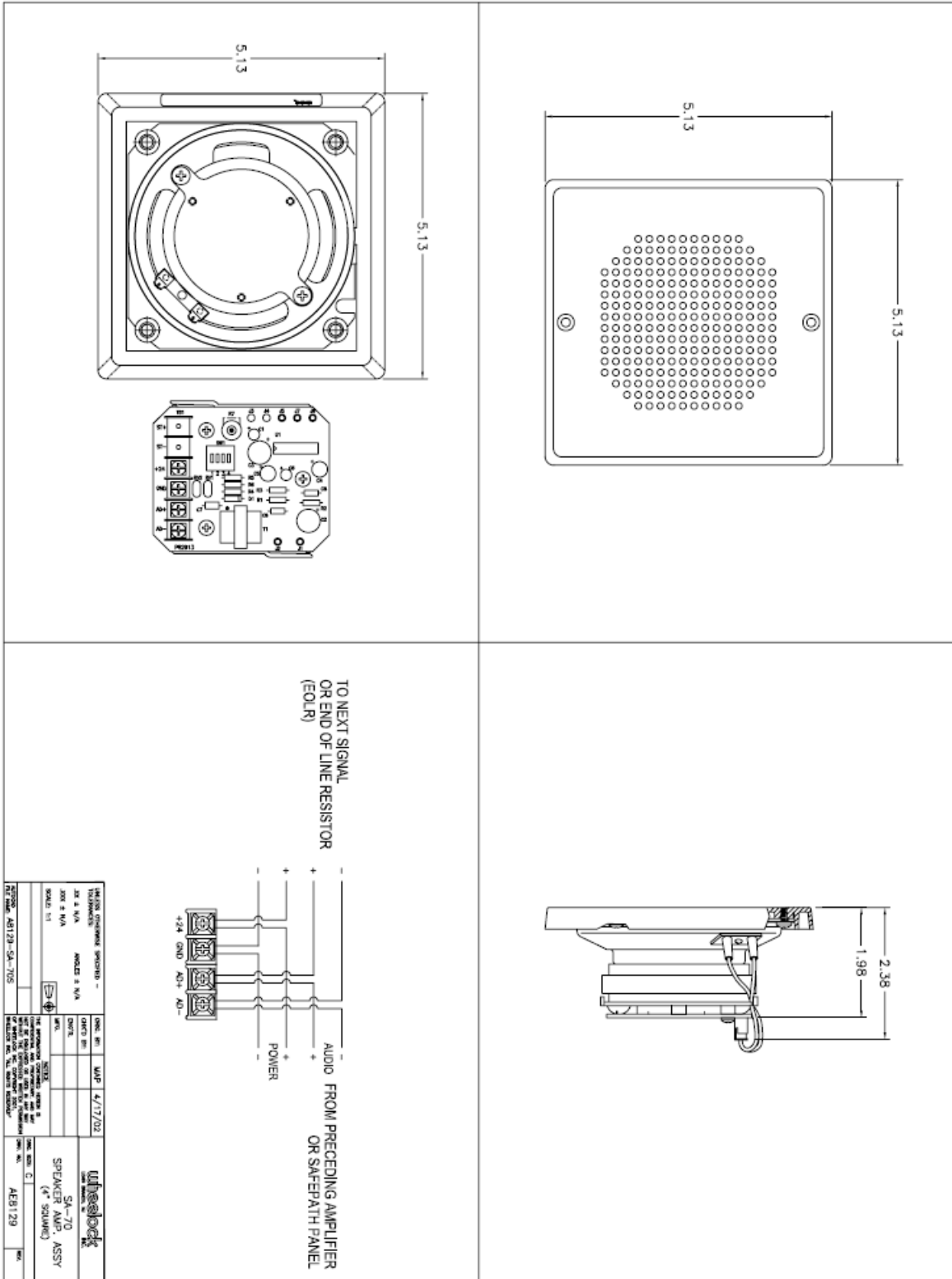
Test Conditions:

- Optical loss all fiber +0.5 dB passive.
- Room temperature 25° C ± 5° (77° F ± 9°).
- 77 CW carriers (NTSC frequency planning) +200 MHz digital.
- Typical value ± 0.5 dB measurement uncertainty.

SUGGESTED FIRE ALARM ANNUCIATOR EQUIPMENT (HORN STROBE)



SUGGESTED FIRE ALARM ANNUCIATOR EQUIPMENT (SPEAKER ASSEMBLY)



SUGGESTED PUBLIC ANNOUNCEMENT (PA) SYSTEM EQUIPMENT

V-1040 INSTALLATION INSTRUCTIONS FOR CLEAN ROOM CEILING SPEAKER

The Valcom Ceiling Speaker, V-1040 is a self-amplified and capable of reproducing voice paging in clean room environments. The V-1040 has a screwdriver adjustable volume control located on the 1 watt amplifier circuit board. The V-1040 has an 8-inch speaker. The speaker requires -24VDC, 50mA (1-power unit). The speaker features the following, large rubber o-ring to seal the grille to the ceiling, rubber washers for all mounting hardware and a polycarbonate dust shield located between the speaker and the grille.

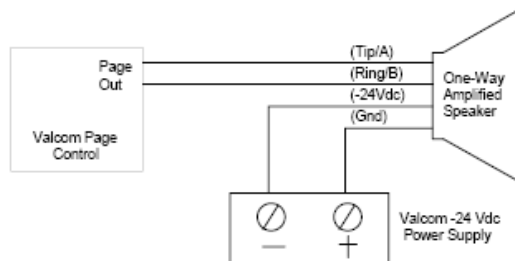
Dimensions/Weight

- V-1040 13.00"Dia. x 3.00"D (33.02cm Dia. x 7.62cm D) 2.5 lbs. (1.13kg)

Coverage

The area covered by a ceiling speaker is determined by the height of the ceiling. If ceiling height is 8 feet, the speaker will cover 256 sq. ft. With a ceiling height of 10 feet, the speaker will cover 400 sq. ft. If the ceiling is 20 feet high, the speaker will cover 1600 sq. ft.

Connections



Refer to Figure 1 for audio and electrical connections. Category 3 24 AWG structured cable may be used for all connections.

NOTE: Do not connect this speaker directly to a 25/70/100 Volt amplifier as damage to both the amplifier and speaker may occur. A V-1095 may be used to allow the use of Valcom self-amplified speakers on 70V speaker lines.

FIGURE 1: TYPICAL CONNECTIONS

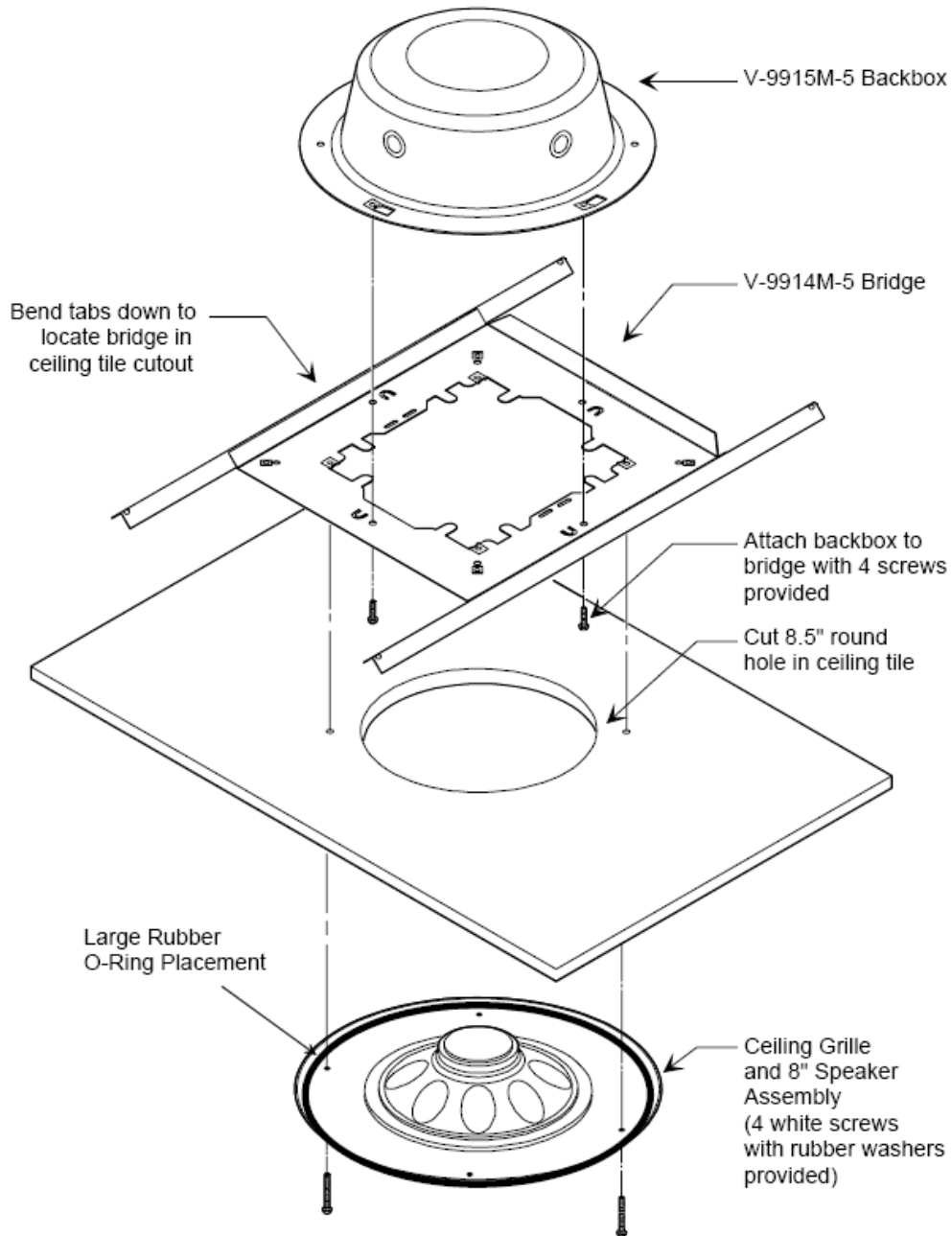
Installation

Suspended Ceiling Installation

After determining the speaker location and referring to Figure 2 cut an 8.5" diameter hole in the ceiling tile. Attach the backbox to the bridge with the four screws provided and position the assembly on the back of the ceiling tile. **Before continuing speaker installation using a small screwdriver set Volume Control to 2/3 rotation.** Place the large rubber O-ring on the back of the speaker assembly and using the four screws equipped with washers and O-rings mount the speaker assembly to the bridge/backbox assembly. *Do not over-tighten the speaker mounting screws. Hand-tighten only. For a proper seal the large O-ring should compress slightly. It is not necessary for the edge of the metal grille to touch the ceiling tile for a proper seal.* Refer to Figure 2.

SUGGESTED PUBLIC ANNOUNCEMENT (PA) SYSTEM EQUIPMENT

FIGURE 2: V-1040 INSTALLATION INSTRUCTIONS



Best Practices



Information Management: Security of Building Plans

*A joint advisory of
the American Institute of Architects, the National Society of Professional Engineers
and the U.S. General Services Administration.*

The AIA collects and disseminates Best Practices as a service to AIA members without endorsement or recommendation. Appropriate use of the information provided is the responsibility of the reader.

REQUESTS FOR BUILDING PLANS

From time to time, design and engineering firms receive requests for building plans that appear unusual due to the structures identified in the requests, the type of information solicited, or the persons or organizations making the request. While most requests are likely to be routine and legitimate, design firms are advised to exercise reasonable caution and good judgment in reviewing each request before providing documents or plans to persons or organizations unknown to them.

TO REPORT SUSPICIOUS REQUESTS

The U.S. Federal Bureau of Investigation (FBI) advises design firms to heighten their awareness and to immediately report any suspicious requests to the appropriate local FBI field office and to the National Infrastructure Protection Center, at FBI headquarters. Please use the attached Building Plan Request Reporting Form for this purpose.

Contact information for FBI field offices can be found in local telephone directories and at:

<http://www.fbi.gov/contact/fo/fo.htm>

The National Infrastructure Protection Center can be reached:

by fax: (202) 323-2079

by email: nipc.watch@fbi.gov

Again, please note that all reports should be sent directly to BOTH your local FBI field office and to the National Infrastructure Protection Center. If the report involves a U.S. General Services Administration building or project, a copy of the report should also be sent to:

Criminal Investigation Division
Federal Protective Service
Attention: L. Phelps
GSA Building
18 & F Streets, NW
Washington, DC 20405
(202) 501-0793 (phone)
(202) 219-9832 (fax)

Building Plan Request Reporting Form

A number of firms from the design and engineering community are reporting recent or past requests for building plans that, in light of the attacks of September 11, 2001, appear unusual due to the structures identified in the requests or the type of information solicited. While most requests are likely to be routine and legitimate, it is appropriate to exercise reasonable caution and good judgment in reviewing each request before providing documents or plans to unknown persons or organizations. The U.S. General Services Administration (GSA), The American Institute of Architects, and the National Society of Professional Engineers are providing this form to assist design and engineering professionals who deem a request for plans to be unusual and who wish to report such a request to authorities for investigation.

Information on Request

Today's date

Date of request for plans

Name of individual / organization requesting plans

Address

Caller's Phone (office)

Caller's Phone (home)

Caller's Email

Caller's Fax

Name of building or facility for which plans were requested

Address of building

This building / facility is a:

- Government building (federal, state or local)
- Military installation
- Commercial / residential building
- Entertainment / athletic facility
- Airport
- Other _____

Please comment on why the request seems unusual.

Has the individual or organization made previous requests for information? Yes No If yes, please explain.

Firm/Individual Reporting Request

Name of individual reporting request

Name of firm

Address

Phone (office)

Phone (home)

Email

Fax

Type of firm:

- Architecture
- Engineering
- Interior Design
- Other _____

Submitting Report

Please immediately send a completed report by fax or email to the appropriate local FBI field office. Consult <http://www.fbi.gov/contact/fo/fo.htm> or a local phone directory for specific contact information.

Also, please send the report by fax (202-323-2079) or email (nipc_watch@fbi.gov) to the National Infrastructure Protection Center at FBI headquarters.

If the report involves a GSA building or project, please send a copy of the report to:

Criminal Investigation Division
Federal Protective Service
Attention: L. Phelps
GSA Building
18th & F Streets, NW
Washington, DC 20405
Phone: 202-501-0793
Fax: 202-219-9832