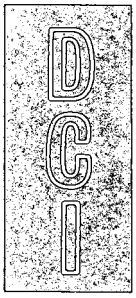
NFIB/NFIC-9.1/47



DIRECTOR
OF
CENTRAL
INTELLIGENCE

U.S. Intelligence Community Physical Security Standards for Sensitive Compartmented Information Facilities

U.S. INTELLIGENCE COMMUNITY POLICY STATEMENT ESTABLISHING PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs) [1]

(Effective 23 April 1981)

Physical security standards are hereby established governing the construction and protection of facilities for storing and processing Sensitive Compartmented Information (SCI) [2] which requires extraordinary security safeguards as prescribed in pertinent national directives. These regulations also cover electric or electronic equipment located in SCIFs. Compliance with these standards is mandatory for all facilities established after the effective date above, including any renovation of existing facilities insofar as the renovation will permit reasonable and practical upgrading. It is not intended that existing, previously approved facilities be modified to conform to these standards. Facilities which meet these standards are satisfactory for the storage of all SCI.

It is recognized that there may be instances in which circumstances constitute a threat of such proportion that it can only be offset by the most stringent security arrangements. Conversely, there may arise those instances in which time, location, condition of use of the material, or other unforeseen factors may render full compliance with these standards unreasonable or impossible. Situations such as the foregoing are to be referred to the accreditation authority as far in advance as possible in order that full and timely consideration may be given to a request for deviation from the standards. When these standards are waived for an SCIF, the accreditation authority who waives them will inform the SCIF Manager of the areas of the SCIF that do not meet standards and what changes are necessary before the SCIF will meet them. For contractor operated SCIFs, waivers are valid no longer than the term of the contract. The fact of a waiver condition will be made known by the cognizant element to other components desiring to share the facility.

All facilities must be accredited before SCI may be stored in them. The procedures for establishment and accreditation of SCIFs are prescribed in applicable national directives.

---

[1] This supersedes USIB-D-9.1/20 dated 30 April 1973, "Policy Statement—USIB Physical Security Standards for Compartmented Information Facilities"

[2] "Sensitive Compartmented Information" (SCI) as used in this policy statement means all classified information and materials bearing Intelligence Community special access controls formally limiting access and dissemination. This term does not include Restricted Data as defined in Section II, Atomic Energy Act of 1954, as amended.

PHYSICAL SECURITY STANDARDS FOR SENSITIVE COMPARTMENTED INFORMATION FACILITIES (SCIFs)

TABLE OF CONTENTS

SECTION I

DEFINITIONS

1. **Access Control System, Unattended**—An electronic, electromechanical or mechanical system designed to identify and/or admit personnel with properly authorized access to the secure area. Identification may be based on any number of factors such as a sequencing of a combination, special key, badge, fingerprints, signature, voice, etc. These systems are for personnel access control only and are not to be used for the protection of stored materials.

2. **Acoustic Security**—Those security measures designed and used to deny aural access to classified information.

3. **Administrative/Service Areas**—Those identified areas within an accredited SCIF where no storage, handling, discussion and/or processing of SCI is allowed.

4. **Alarm Door Switch**—A balanced magnetic switch so designed and installed that opening the door or introducing an outside magnetic force will cause an alarm to be generated.

5. **Alert Security System**—A security system which has a local signalling device to alert persons inside a facility that someone has come in through an entrance.

6. **Authorized Personnel**—Any person who is fully cleared and briefed for SCI and has been granted access to the SCIF.

7. **Class A Electronic Line Supervision**—A system which transmits over wire a pseudo-random generated tone or tones or digital type modulation. (This system exceeds the previous "High Line Security" system requirement.)

8. **Class B Electronic Line Supervision**—A system which transmits over wire a digital or tone type modulation. (This system is equivalent to the previous "High Line Security" system requirement.)

9. **Class C Electronic Line Supervision**—A system, AC or DC, which is wire transmitted. (This system is equivalent to the previous "Standard Line Security" system requirement.)

10. **Closed Storage**—The storage of SCI in properly secured GSA approved security containers within an accredited SCIF while such facility is not occupied by authorized personnel.

11. **Continuous Operations**—This condition exists when a facility is manned 24 hours every day by not fewer than two appropriately cleared personnel who have the continuous capability of detecting unauthorized entry into the SCIF. Positive identification and access control must be maintained at all entrance points not fully secured.

12. **Continuous Personnel Access Control**—An access control system where access to the building is continuously controlled by a cleared individual.

13. **Controlled Area**—Any area to which entry is subject to restrictions or control for security reasons.

14. **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.

15. **Forced Entry**—Unauthorized entry into an SCIF or security container in a manner in which evidence of such entry is easily discernible.

16. **Guard**—A properly trained and equipped individual whose duties include the protection of an SCIF. Guards whose duties require direct access to an SCIF, or patrol within an SCIF, must meet the clearance criteria in Director of Central Intelligence Directive No. 1/14, but need not be indoctrinated for access to SCI.

17. **High Line Supervision**—See Class A and Class B Electronic Line Supervision.

18. **Intrusion Detection System**—A security alarm system consisting of various types of alarms (vibration, capacitance, volumetric, etc.) to detect the unauthorized intrusion into a facility.

19. **Non-Discussion Area**—A clearly defined area within an SCIF where classified discussions are not authorized. All such areas shall be clearly marked.

20. **Open Storage**—The storage of SCI in other than GSA approved security containers within an SCIF when it is not occupied by authorized personnel.

21. **Optical Security**—Those security measures designed and used to deny visual access to classified objects, documents, rooms, etc.

22. **SCI Facility (SCIF)**—An accredited area, room, group of rooms, or installations where SCI may be stored, used, discussed and/or electronically processed.

23. **SCI Security Control System**—A system which provides for the security control of special access program information within the category of National Security Information (NSI) called National Foreign Intelligence (NFI).

24. **Secure Area**—An accredited facility which is used for storing, handling, discussing, and/or processing of SCI.

25. **Secure Working Area**—An accredited facility which is used for handling, discussing and/or processing of SCI but where SCI shall not be stored.

26. **Senior Intelligence Officer (SIO)**—Those senior principals and observers on the National Foreign Intelligence Board who head intelligence organizations or intelligence producing agencies within the Intelligence Community.

27. **Sound Groups**—Sound transmission attenuation groups (ratings measured in decibels-db) established to satisfy the acoustical security requirements of SCIFs.

28. **Sound Transmission Class** (STC)—The rating used in architectural considerations of sound transmission loss such as those involving walls, ceilings, and/or floors.

29. **Standard Line Supervision**—See Class C Electronic Line Supervision.

30. **Surreptitious Entry**—The unauthorized entry into an SCIF or security container in a manner in which evidence of such entry is not readily discernible.

31. **Tactical or Combat Operations**—Operations which are conducted under combat or simulated combat conditions and which must provide for a mobile or semi-permanent environment.

32. **Technical Surveillance Countermeasures (TSCM) Surveys and Inspections**—A thorough physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and related physical security weaknesses.

33. **Temporary Secure Area (TSA)**—A temporarily accredited facility which is used for storing, handling, discussing, and/or processing of SCI.

34. **Temporary Secure Working Area (TSWA)**—A temporarily accredited facility which is used for handling, discussing, and/or processing of SCI, but where SCI shall not be stored.

35. **Two-Person Rule**—As a matter of policy, SCI Control Facilities (SCIFs) should be staffed with sufficient people to deter unauthorized copying or illegal removal of SCI. SCIF designated communication centers, document control centers (registries), and like facilities that handle or store quantities of SCI must be manned while in operation by at least two appropriately indoctrinated persons in such proximity to one another as to provide mutual support in maintaining the integrity of the facility and the material stored therein. The granting by an SIO of exceptions to this policy will be made a matter of record and should involve consideration of the proven reliability and maturity of the persons involved; the volume, variety and sensitivity of the holdings in the facility; and whether or not the persons involved are subject to periodic polygraph examinations as a condition of access. Exceptions for communications centers, document control centers, and the like, should be granted in only extraordinary circumstances. Routine work by a lone individual in any SCIF is to be avoided. Contractors will provide two person occupancy in all SCIFs not specifically exempted by the SIO of the Government sponsor.

36. **Vault**—A maximum protection accredited facility which is used for storing, handling, discussing, and/or processing of SCI.

37. **Volumetric Detection System**—An alarm system which detects movement or human presence within a protected area.

SECTION II

PERIMETER CONSTRUCTION CRITERIA FOR SCI FACILITIES

1. **GENERAL**—The construction of and the physical security protection for an SCI Facility (SCIF) must prevent the visual, acoustic, technical and physical access to or compromise of classified information. It must also permit detection of forced or surreptitious entry of the facility. The criteria for the construction of perimeters are governed by whether the facility is in the United States or not, and whether it is located at, above or below ground level according to the following situations: Open Storage, Closed Storage, Continuous Operations, Secure Working Areas, and Non-Discussion Areas.

2. **COMMON CRITERIA**—Certain criteria, however, are common to every facility and apply to all locations and situations. These are set forth as follows:

   A. **AIR VENTS AND DUCTS**—All air vents, ducts, and similar openings that pass through a facility's perimeter will be protected and equipped as prescribed below:

      (1) Sound protection—All openings will be sound baffled where appropriate to meet the requirements of Sound Transmission Class (STC) 45 or better (not required for Non-Discussion Areas).

      (2) Nonconductive Section—All ducts must have a nonconductive section installed at the perimeter of the SCIF.

      (3) Physical protection—All openings larger than 90 square inches will be protected at the perimeter with the following installed in the order listed, progressing inward from the outer face of the perimeter:

         (a) Hardened steel bars one-half inch in diameter, mounted five inches on center vertically and horizontally and welded at all the intersections.

         (b) An alarm device (not required for Non-Discussion Areas).

         (c) Access ports to facilitate the inspection of any installed security devices and to permit examination of the interior of the vent and duct runs for the presence of unauthorized objects. These access ports will be within the secure perimeter of the SCIF.

   B. **SOUND ATTENUATION**—Except for Non-Discussion Areas, all SCIFs, regardless of location or situation, must meet the specifications for sound attenuation as set forth in Annex C.

   C. **ALARM REQUIREMENTS**—All SCIFs, as defined in Section I, must meet the requirements for security alarms as set forth in Section III.

   D. **DOORS**

      (1) Normally there will be a single controlled entrance to an SCIF. When safety or other considerations require more than one door, only one of the doors will be used as the entrance access control point. The other door(s) will be secondary and secured from the inside with either bars and brackets, or sliding dead bolts, and/or dead bolt panic hardware.

(2) Door requirements for Vaults and Secure Areas will be as stated in Annex A and Annex B, respectively.

(3) The entrance door will be equipped with a permanently mounted approved Group I combination lock and have an inside escape mechanism. The access door will also be equipped with a door closer and may be equipped with an access control device for use as a convenience during working hours. Secondary exit door(s), if required, will be of equal construction as the entrance door and locked as described in D(1) above. Door hinges located on the door exterior will be the nonremovable type with hinge pins peened or otherwise secured to preclude removal.

E. **WINDOWS**—Windows should be permanently sealed. All windows in an SCIF which might reasonably afford optical surveillance of personnel, documents, materials, hardware or activities within the SCIF shall be made opaque or equipped with blinds, drapes, or other suitable coverings which will preclude such surveillance.

3. **SCI FACILITIES IN THE UNITED STATES AT GROUND LEVEL**—SCIFs at ground level must meet the construction criteria set forth herein as they apply to the following situations:

A. **OPEN STORAGE**—Open storage of SCI shall be avoided if possible. When open storage is required, the SCIF must meet either the specifications for vaults set forth in Annex A, or be located in a building that has:

(1) Continuous personnel access control;

(2) A 24-hour guard force capable of responding to an alarm within five minutes or less;

(3) A reserve guard force available to assist the responding guard in an emergency, and
The area is alarmed in accordance with Section III, and the SCIF is constructed as a secure area according to Annex B, paragraph 1A.

B. **CLOSED STORAGE**

(1) The SCIF must meet the specifications of a Secure Area specified in Annex B.

(2) SCI must be stored in GSA approved security containers having a resistance to surreptitious entry equal to or exceeding that of a Class 6 container.

C. **CONTINUOUS OPERATIONS**

(1) The floors, walls, and ceilings in such part of the facility must be constructed of substantial material that provides protection against forced entry.

(2) An adequate security force must be available to respond to the SCIF within five minutes in an emergency.

(3) In an emergency, all SCI must be stored in lockable containers. If the bulk of the material precludes this, then there must be an adequate, tested plan to protect, evacuate, or destroy the material.

D. **SECURE WORKING AREAS**—Perimeter walls, floors, and ceilings may be constructed without regard to the thickness or type of material so long as they will show evidence of attempted forced or surreptitious entry.

4. **SCI FACILITIES IN THE UNITED STATES ABOVE OR COMPLETELY BELOW GROUND LEVEL**—Facilities above or completely below ground level with no ready access to exterior openings must meet the construction specifications set forth herein as they apply to the following situations:

A. **OPEN STORAGE**—Open storage of SCI shall be avoided if possible. When open storage is required, the SCIF must meet either the specifications for secure areas set forth in Annex B, paragraph 1B, or be located in a building that has:

(1) Continuous personnel access control;

(2) A 24-hour guard force capable of responding to an alarm within five minutes or less;

(3) A reserve guard force available to assist the responding guard in an emergency, and

The area is alarmed in accordance with Section III, and the SCIF meets construction specifications in Annex B, paragraph 1A.

B. **CLOSED STORAGE**

(1) SCI must be stored in GSA approved security containers having a resistance to surreptitious entry equal to or exceeding that of a Class 6 container.

(2) The floors, walls, and ceilings must be constructed of substantial, permanent material which provides protection against forced or surreptitious entry and which will offer visual evidence of surreptitious entry. Walls will be attached to floors and true ceilings solidly and permanently.

C. **CONTINUOUS OPERATION**

(1) No alarm or special construction is required other than to meet sound attenuation requirements set forth in Annex C. If there is the possibility of surreptitious entry, however, then alarms and/or barriers as discussed in Section II, paragraph 2, must be used to guard against such penetration.

(2) In an emergency, all SCI must be stored in lockable containers. If the bulk of the material precludes this, then there must be an adequate, tested plan to protect, evacuate or destroy the material.

D. **SECURE WORKING AREAS**—The construction of, and the physical security protection for, a secure working area must provide for the detection of both forced or surreptitious entry of the SCIF, including those areas above false ceilings or below false floors. Perimeter walls, floors, and ceilings may be constructed without regard to the thickness or type of material so long as they will show evidence of attempted forced entry.

5. **SCI FACILITIES LOCATED OUTSIDE THE UNITED STATES**—The criteria for SCIFs outside the United States are the same as those for SCIFs within the United States except as follows:

A. **OPEN STORAGE**

(1) No waiver shall be granted for the vault construction of an SCIF approved for open storage.

(2) No waiver shall be granted for the secure area construction requirement of an SCIF approved for open storage.

(3) Open storage of SCI will be permitted only for material which is of a size or configuration that precludes its being stored in the largest GSA approved security container available. All other SCI must be stored in GSA approved security containers having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.

B. **CLOSED STORAGE**

(1) The SCIF must meet secure area construction specifications as listed in Annex B, paragraph 1B.

(2) All SCI controlled material shall be stored in GSA approved security containers having a rating for both forced and surreptitious entry equal to or exceeding that afforded by Class 5 containers.

C. **CONTINUOUS OPERATIONS**

(1) The SCIF must meet secure area construction specifications as listed in Annex B, paragraph 1B.

(2) In an emergency, all SCI must be stored in GSA approved security containers, or the SCIF must have an adequate, tested plan to protect, evacuate or destroy the information.

SECTION III

SECURITY ALARM SYSTEMS

1. **PURPOSE**—The purpose of an alarm system is to detect an intrusion or attempted intrusion into an SCIF and to notify appropriate personnel. Whenever these requirements state a class of alarm system, they are referring to the method of transmitting an alarm signal.

2. **CLASSES OF ELECTRONIC LINE SUPERVISION**

   A. **CLASS A**—Pseudo-random digital and tone-wire transmitted preferred. (Exceeds previous "High Line Security" requirement.)

      (1) These systems will transmit over wire a pseudo-random generated tone or tones or digital type modulation. These systems will use either an interrogation and reply scheme or a synchronization scheme. The signal between the protected premises and the monitor location shall not repeat itself within a six month period. A line supervision alarm signal shall cause a lock-in condition which shall be transmitted to the monitor location in not more than 30 seconds. If the above conditions cannot be met, then a UL approved system with commercial Grade A service and Grade AA transmission will be acceptable.

      (2) It shall not be possible to compromise Class A systems by the use of resistance, voltage or current substitution techniques.

   B. **CLASS B**—Digital and tone-wire transmitted preferred. (Formerly described as High Line Security.)

      (1) The systems using digital or tone type modulation over transmission lines shall use an interrogation and reply scheme. The signal technique used for the interrogation shall be different than that of the reply. Each line supervision alarm signal shall cause a lock-in condition which shall be transmitted to the annunciator in not more than 90 seconds. If the above conditions cannot be met, then a UL approved system with Grade B commercial service and Grade A transmission will be acceptable.

      (2) It shall not be possible to compromise Class B system by the use of resistance, voltage, or current substitution techniques. The circuits and methods employed shall be highly immune to transmission line noise, such as crosstalk, hum, transients, and the like.

   C. **CLASS C**—AC and DC—Wire Transmitted. (Standard Line Security.) The Class C circuit supervisor units shall provide an alarm response in the annunciator in not more than one second as a result of the following changes in normal transmission line current:

      (1) Five percent or more in normal line signal when it consists of direct current from 0.5 milliamperes through 30 milliamperes.

      (2) Ten percent or more in normal line signal when it consists of direct current from 10 microamperes to 0.5 milliamperes.

      (3) Five percent or more of any component or components in a complex signal upon which the security integrity of the system is dependent. This tolerance will be

applied for frequencies up to 100Hz. Component as used in this specification means AC or DC voltage or current, AC phase, or frequency duration.

(4) Fifteen percent or more of any component or components in a complex signal upon which the security integrity of the system is dependent. This tolerance will be applicable for all frequencies above 100Hz. Component as used in this specification means an AC or DC voltage or current, AC phase, or frequency duration.

3. **FACTORS**—The factors that determine whether or not an SCIF shall have an alarm or alert system are:

A. **LOCATION**

(1) Within the United States.

(2) Outside the United States.

B. **TYPE OF OPERATION**

(1) Continuous.

(2) Noncontinuous.

4. **ALARM REQUIREMENTS**

A. **SCIFs located within the United States**

(1) Continuous Operation SCIFs are not required to have an alarm system unless there exists a possibility of surreptitious entry. This determination shall be made by the SIO.

(2) Noncontinuous Operation SCIFs shall be alarmed and have a Class A line supervision system if the transmission signal leaves the SCIF and traverses an uncontrolled area.

(3) Noncontinuous Operation SCIFs shall be alarmed and have a Class A or Class B line supervision system if the transmission signal does not leave the controlled area containing the SCIF.

(4) If an SCIF cannot meet the requirements of (1), (2), or (3) above due to unavailability of transmission and/or monitoring facilities, then the SCIF must be protected by an alarm system utilizing a Class C line supervision system and which has an external UL approved bank vault type bell. Approval for the substitution of a Class A or Class B line supervision system by the above mentioned Class C line supervision system can only be granted by the SIO.

B. **SCIFs located outside the United States**—All SCIFs located outside the United States, regardless of the type of operation, shall have an alarm system or alert system. Either system must be monitored by U.S. citizens.

(1) Continuous Operation SCIFs shall have, as a minimum, an alert system. If there exists a possibility of surreptitious entry, appropriate alarms will be installed. This determination will be made by the SIO.

(2) Noncontinuous Operation SCIFs shall be alarmed and have a Class A line supervision system.

(3) SCIFs for which the two-person rule has been waived should have, in addition to an alarm or alert system, a panic system for emergency notification to an outside cognizant individual or other facility to provide immediate response.

5. **ALARM SYSTEM**

   A. Equipment shall be UL approved (or equivalent).

   B. Areas of the SCIF between the floor and ceiling shall be protected by volumetric sensors.

   C. If an SCIF has a false ceiling or floor which provides a means for surreptitious entry, then one of the below listed methods must be used to protect that area:

      (1) A separate alarm system covering the area between the false and true ceiling or false and true floor.

      (2) Expanded metal (9-11 gauge).

   D. Perimeter doors will be protected by balanced magnetic switches.

   E. All windows will be protected by an alarm system.

   F. Emergency exits and secondary doors shall be on a separate zone from the volumetric and main entrance sensors within the same SCIF.

   G. Every SCIF shall be on a separate zone.

   H. If an SCIF consists of more than 6 rooms, or more than 5,000 square feet, then it shall be protected by two or more alarm zones as determined by the cognizant security authority.

   I. All control units will be located within the protected area.

   J. All alarm systems will be tested monthly, i.e., doors opened and volumetric sensors walk tested. Detailed test procedures will be prepared which outline the required tests by the SCIF Manager.

   K. All components shall be installed in a manner to prevent access or removal from a location external to the protected zone.

   L. All alarm systems shall be capable of operating from commercial AC power. In the event of commercial power failure, provisions will be made for automatic switchover to emergency power, and back to commercial power without causing an alarm. A signal will be presented to the monitor location indicating when the system has lost all power. When batteries are used for emergency power, they will be maintained at full charge by automatic charging circuits. Emergency power must be capable of operating the system for a minimum of four hours.

   M. Volumetric sensors employed in the alarm system must be placed so that the most likely intruder motions are detected.

   N. All perimeter sensors and control units will be equipped with tamper detection.

6. **ALERT SYSTEM**—An alert system shall consist of balanced magnetic switches or other appropriate sensors on all entrances. These sensors shall be connected to a signaling device through a closed loop to a latching relay. Neither the signaling device, relay or wire connecting the switches shall leave the SCIF.

SECTION IV

TELEPHONE AND INTERCOMMUNICATIONS EQUIPMENT

1. **CONCEPT**—Unsecure telephones installed in areas where SCI is discussed and/or processed, present an unacceptable threat unless particular attention is paid to applying effective countermeasures. The most effective countermeasure is the exclusion of telephones and associated wire runs and equipment from SCIFs. Telephones and associated wire runs and equipment are therefore prohibited in SCIFs except where operationally justified.

2. **PROTECTIVE MEASURES**—If telephones are permitted within an SCIF, the protective measures outlined below must be applied:

   A. Cable/wire control.

      (1) All telephone wires must enter the SCIF through one opening. Each conductor will be accurately accounted for from the point of entry. The accountability will identify, through labeling or log/journal entries, the current precise use of every conductor. This accountability applies to excess conductors which must also be terminated at the point of entry and connected to appropriate connector blocks and grounded.

      (2) When SCIFs employ dedicated key telephone or computerized systems, the system shall be installed within the secure perimeter of the SCIF and restricted to such use.

   B. Isolation. The telephone instrument must be effectively isolated from all incoming lines when the telephone is not in use, i.e., in the "on-hook" condition. The two approved methods of achieving isolation are listed below:

      (1) Manual disconnect. Each instrument must be fitted with a plug and jack arrangement so that the telephone can be manually disconnected at all times when not in use. This method requires the incorporation of an audible alarm in the "on-hook" condition to warn users to remove the plug upon completion of calls. (Attachment 1, Section IV, is a diagram of an approved installation method.)

      (2) Automatic disconnect. Any Telephone Security Panel (TSP) approved automatic disconnect system may be used.

   C. Handsets. All telephones will be equipped with a TSP approved handset.

   D. Ringers. Signalling of incoming calls will be accomplished by one of the following procedures:

      (1) In SCIFs where the Key Service Unit (KSU) is installed, no special signalling apparatus is required if the KSU includes a local ring generator and is wired for common audible signalling. Any ringer or buzzer may be used.

      (2) In SCIFs where KSU is not used, a TSP approved signalling device will be used.

3. **SPECIALIZED EQUIPMENT**—The installation of specialized telephone equipment, such as telephone answering devices or speaker phones, within an SCIF is prohibited.

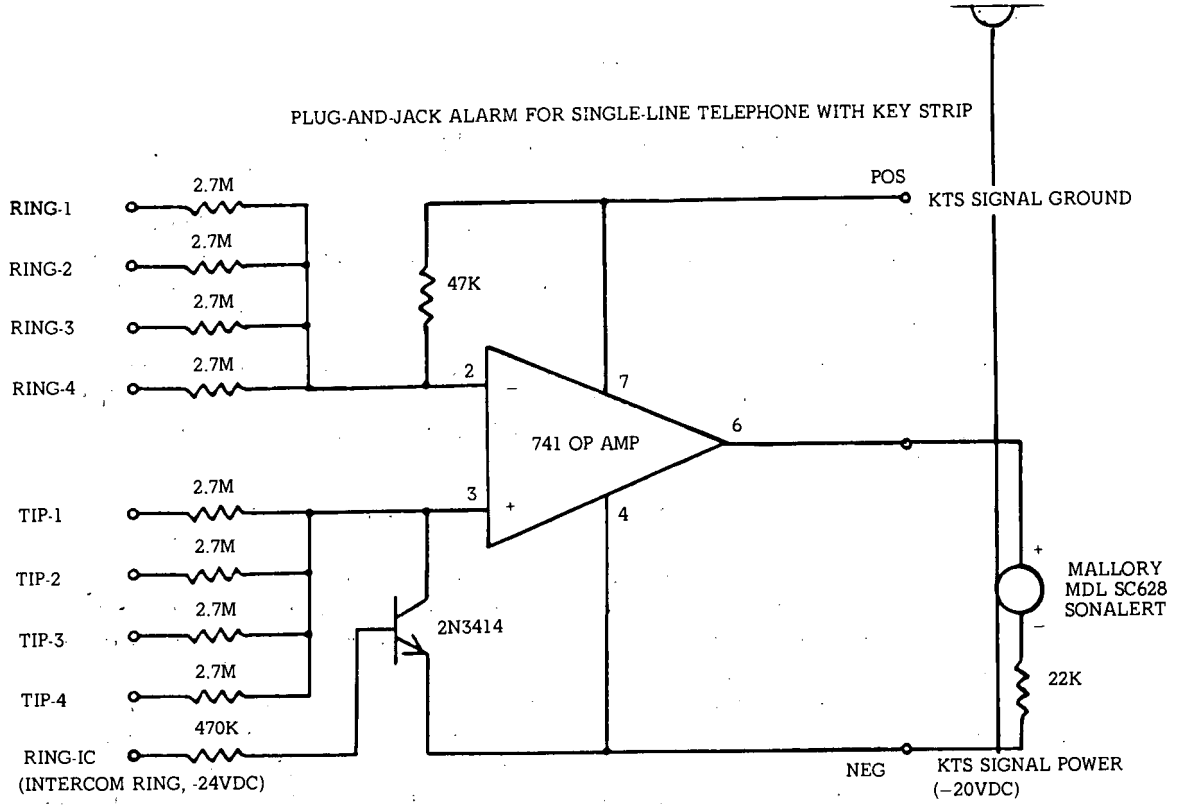
4. **INTERCOMMUNICATIONS EQUIPMENT**—The installation of intercommunications systems within SCIFs is prohibited except where operationally justified and installed according to the guidance below:

   A. If a dial-type intercommunications system capability is engineered into the approved telephone system, no further action is required provided that the system is installed according to paragraphs one through three above.

   B. If a separate telephone, dial type system is installed, no station or wiring will be located outside the SCIF and all wiring will be installed in a manner that permits visual observation of the complete wire run, or installed within electromagnetic tubing (EMT).

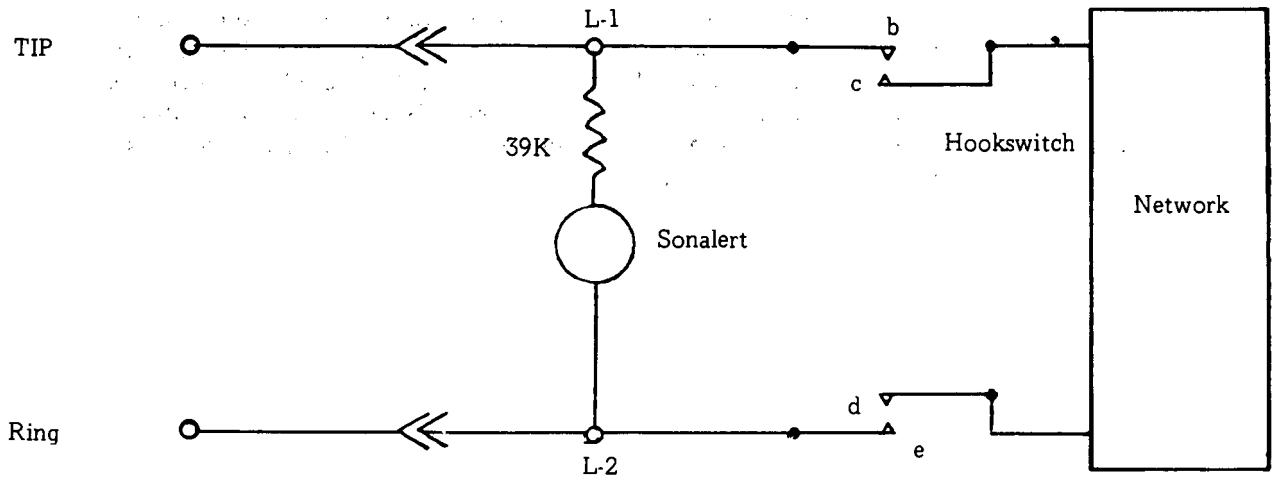
ATTACHMENT # 1

PLUG-AND-JACK ALARM FOR SINGLE-LINE TELEPHONE WITH KEY STRIP



CURRENT REQUIREMENT FROM KTS SIGNAL POWER : ON-HOOK 1.7 mA, OFF-HOOK 1.1 mA, EACH SONALERT ADDS 1 mA.

SINGLE-LINE TELEPHONE, ANY TYPE



<<< = Plug-and-Jack connections

SECTION V

MISCELLANEOUS PHYSICAL SECURITY REQUIREMENTS

1. **GENERAL:** With the increased handling of SCI in facilities which do not have strictly enforced personnel access programs, which do not have a controlled area surrounding the SCIF, and/or which house non-government personnel, efforts shall be made to ensure that all security safeguards are strictly employed.

2. **ACCESS CONTROLS:** SCIFs shall be afforded personnel access controls to preclude entry by unauthorized personnel. Non-SCI indoctrinated personnel entering an SCIF shall be continuously escorted by an SCI indoctrinated employee who is familiar with the security procedures of that SCIF.

3. **TEMPORARY SECURE AREA (TSA)**—A TSA shall be equipped with GSA approved security containers and SCI shall be stored therein. The entrance(s) to this facility shall be alarmed with balanced magnetic switches and an approved volumetric alarm system. If such a facility must also be used for the discussion of SCI, a TSCM shall be conducted periodically on a random basis during the operation of this temporary facility and personnel access shall be limited to those employees who possess the appropriate SCI access(es). Such a facility shall be accredited on a temporary basis by the Intelligence Community agency/department SIO for a non-renewable period of 6 months or less. A shipboard facility may be accredited on a temporary basis for a nonrenewable period not to exceed the duration of the mission. No special construction is required other than to meet sound attenuation requirements.

4. **TEMPORARY SECURE WORKING AREA (TSWA)**—The entrance will be controlled, and access limited to persons having the clearance for which the area has been approved during the entire period the TSWA is in use. Approval for using such areas must be obtained from the SIO of the next higher level within appropriate SCI channels, setting forth room number(s), building, location, specific security measures employed during usage as well as during other periods, and purpose of such usage. These areas will 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. If such a facility must also be used for the discussion of SCI, a TSCM shall be conducted periodically on a random basis during the operation of this temporary facility.

SECTION VI

TACTICAL OR COMBAT OPERATIONS AND PORTABLE/MOBILE SCIFs

1. Security standards for tactical or combat operations can only prescribe the minimum requirements, since each situation differs. Situation and time permitting, the minimum standards below will be improved upon, using the security considerations and requirements for permanent secure facilities as an ultimate goal. When available, permanent type facilities shall be used.

2. For tactical or combat conditions, a continuous 24 hours a day operation is mandatory. Every effort must be made to obtain all necessary support from the headquarters served (e.g., security containers, vehicles, generators, fencing, automatic weapons, etc.)

3. Recognizing that tactical/combat operations, as opposed to operations within a fixed installation, are of the type which may be considered least secure, the following minimum physical security requirements must be met:

   a. The SCIF shall be physically located well within the supported headquarters area preferably adjacent to the Command/Tactical Operations Center.

   b. The SCIF shall be located within a controlled area with the perimeter of the controlled area clearly marked.

   c. The perimeter of the controlled area shall be guarded continuously (24 hours) by walking or fixed guards to provide observation of the entire controlled area. Guards shall be armed with weapons and ammunition prescribed by the supporting officer in charge.

   d. Access into the area will be restricted to a single point of entry.

   e. The entrance to the controlled area will be guarded on a continuous basis.

   f. A minimum of two appropriately indoctrinated personnel shall be within the facility at all times.

   g. Emergency destruction and evacuation plans will be kept current and tested periodically.

   h. When not in use, SCI shall be stored in lockable containers.

4. The major concern in the use of portable/mobile SCIFs in a semipermanent configuration is that the material stored therein or the facility itself does not receive a lesser degree of protection than that afforded in a strictly tactical operations environment or a permanent facility.

   a. When portable type vans and shelters are operated in a semipermanent environment, they must be operated and protected according to this Section or Sections II and III of this publication. In some instances it may be necessary to combine some security requirements of this Section and some in Sections II and III in order to meet operational requirements and still maintain minimum physical security standards.

   b. Due to the numerous variables in use, configuration, guard response, location, construction, and type of storage, portable SCIFs under this paragraph will be evaluated and accredited on a case-by-case basis.

ANNEX A

VAULT SPECIFICATIONS

1. **CONSTRUCTION CRITERIA:**

   A. **Reinforced concrete construction:**

   Walls, floor, and ceiling shall be a minimum thickness of 8 inches of reinforced concrete. The concrete mixture shall have a compressive strength rating of at least 3,000 PSI. Reinforcing will be accomplished with steel reinforcing rods, a minimum of ⅝" diameter, positioned centrally in the concrete pour and spaced horizontally and vertically 6 inches on center; the 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.

   B. **Steel-lined construction:**

   Where unique structural circumstances do not permit concrete construction of a Vault, construction will be of steel alloy plate, a minimum of $^{3}/_{16}$" thick. The steel selected will be a low carbon alloy type, such as U.S. Steel T-1, having characteristics of high yield and tensile strength. (If alloy-type steel is not available, normal structural steel may be used, but in a minimum thickness of ¼"). 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 contiguous floor and ceiling of reinforced concrete, they must be firmly affixed for a depth of one-half the thickness of the floor and ceiling. If the floor and/or ceiling construction is less than 6 inches of reinforced concrete, then 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.

2. **OPENINGS:**

   A. All Vaults shall be equipped with a GSA approved Class 5 vault door. Normally, a Vault shall have only one door which serves as both entrance and exit from the SCIF. If the "travel distance" from the most remote point in the SCIF to the door exceeds 50 feet, a second door, equal to the original door, must be installed for life safety purposes. Travel distance shall be measured on the floor along the natural path of travel, starting 1 foot from the most remote point, curving around any corners or obstructions, and ending at the entrance doorway. When an SCIF has more than one door, only one should be used for normal business.

   B. Utility openings required for air-conditioning ducts, exhaust fans, and the like, normally shall not exceed 90 square inches and need not be barred or alarmed. (See Section II, paragraph 2A). Utility openings which must exceed 90 square inches shall be justified by the requestor and approved in writing by the SIO. Approved openings which exceed 90 square inches shall be barred with ½" diameter steel rods, placed 5 inches on center vertically and horizontally, welded at the intersections and either securely imbedded into the SCIF wall to a minimum depth of 3 inches or be welded to adjacent steel plates. If excessive moisture is present in the vent opening, stainless steel bars ½" in diameter may be used instead of the normal steel bars; the stainless steel bars must be affixed in the same manner as normal steel bars.

C. Where building codes require that a Vault entrance meet a specified fire rating, a vestibule should be formed on the outside of the entrance and a fire door of the required rating should be installed in addition to the approved vault door. There shall be no windows in a Vault.

3. **MINIMUMS:**

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

ANNEX B

SECURE AREA SPECIFICATIONS

1. **CONSTRUCTION CRITERIA:**

   A. **Secure Area Located Within the United States:** Walls will be reinforced slab to slab with 9-11 gauge expanded steel affixed to supporting members of equal or greater thickness. No other special construction of the SCIF is required so long as the floors, walls and ceilings are constructed of substantial, permanent material which provides protection from surreptitious entry and will offer visual evidence of forced entry. Exterior walls will be attached to floors and true ceilings solidly and permanently.

   B. **Secure Areas Located Outside the United States:** ~~(and stateside Secure Areas with waivers)~~

      (1) Secure Area walls shall be reinforced concrete at least 4 inches thick, or of solid masonry (stone or brick) at least 8 inches thick. Any wall not meeting the above specifications shall be reinforced on the inside with steel plate not less than ⅛" thick. The plates at every vertical joint are to be affixed to vertical steel members of a thickness not less than that of the plate. The vertical plates shall be spot welded to the vertical members by applying a 1 inch long weld every 12 inches; meeting of the plates in the horizontal plane shall be continuously welded. Walls of hollow masonry (blocks and tiles) are not considered adequate and must be reinforced.

      (2) The floor and ceiling of the room shall be of at least 4 inches of reinforced concrete. Floors and ceilings not meeting this criterion must be reinforced with steel plating ⅛" thick. Floor and ceiling reinforcement must be securely affixed to the walls with steel angles welded or bolted in place.

2. **OPENINGS:**

   A. All Secure Areas within the United States shall be equipped with approved Class 6 vault doors, or with locally fabricated doors as indicated in Annex E. Secure Areas overseas shall be equipped with a Class 5 or 6 vault door or an equally strong steel reinforced door and frame. Normally, a Secure Area shall have only one door which serves as both entrance and exit from the SCIF. If the "travel distance" from the most remote point in the SCIF to the door exceeds 50 feet, a second door, equal to the original door, must be installed for life safety purposes. "Travel distance" shall be measured on the floor along the natural path of travel, starting 1 foot from the most remote point, curving around any corners or obstructions, and ending at the entrance doorway. When an SCIF has more than one door, only one should be used for normal business.

   B. Utility openings required for air-conditioning ducts, exhaust fans, and the like, normally shall not exceed 90 square inches and need not be barred or alarmed. (See Section II, paragraph 2A) Utility openings which must exceed 90 square inches shall be justified by the requestor and approved in writing by the SIO. Approved openings which exceed 90 square inches shall be barred with ½" diameter steel rods, placed 5 inches on center vertically and horizontally, and either securely imbedded into the SCIF wall to a minimum depth of 3 inches or be welded to adjacent steel plates. If excessive moisture is

present in the vent opening, stainless steel bars ½" in diameter may be used instead of the normal steel bars; the stainless steel bars must be affixed in the same manner as normal steel bars.

C. Windows:

(1) *Within the United States:* Windows readily accessible will be protected against forced entry and alarmed as described in Section III. If the facility is located in a high crime or risk area, or in one that is subject to civil disorders, steel bars as described in Annex D will be used on the accessible windows in addition to the alarms.

(2) *Outside the United States:* All windows will be protected against forced entry as described in Annex D.

3. **ACCESS:**

Access will be monitored or prevented by any one of those means described in Section V.

ANNEX C

SOUND ATTENUATION CLASSIFICATIONS

1. This Annex provides information to be used as acoustic isolation criteria (voice range only) for construction of SCIFs.

2. The term "Sound Transmission Class" (STC) is used in architectural acoustics to describe the transmission attenuation afforded by various wall materials and other building components expressed in decibels (db). The following transmission attenuation groups have been set up to satisfy the normal security requirements of facilities used for SCI activities.

   A. Sound Group 1 ..... 30 or Better STC. Loud speech can be understood fairly well. Normal speech cannot be easily understood with the unaided human ear.

   B. Sound Group 2 ..... 40 or better STC. Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly if at all with the unaided human ear.

   C. Sound Group 3 ..... 45 or better STC. Loud speech can be faintly heard but not understood. Normal speech is inaudible with the unaided human ear.

   D. Sound Group 4 ..... 50 or better STC. Very loud sounds, such as loud singing, brass music or a radio at full volume, can be heard only faintly or not at all with the unaided human ear.

3. The application of acoustic requirements to SCIFs for various functions is as follows:

Building Areas and Functions	**Sound Group**
Office Space	
Executive suite	3
Private Offices	3
Open Workspace	3
"Lab"	2
Conference Rooms	
Briefing or Conference Rooms	3
Training—Plans Room	3
Conference rooms with movable partition (including movable partition)	3
Auditoriums	
Auditorium with sound reinforcement (No speakers on common wall)	4
Auditorium without sound reinforcement	3
Projection Rooms	3

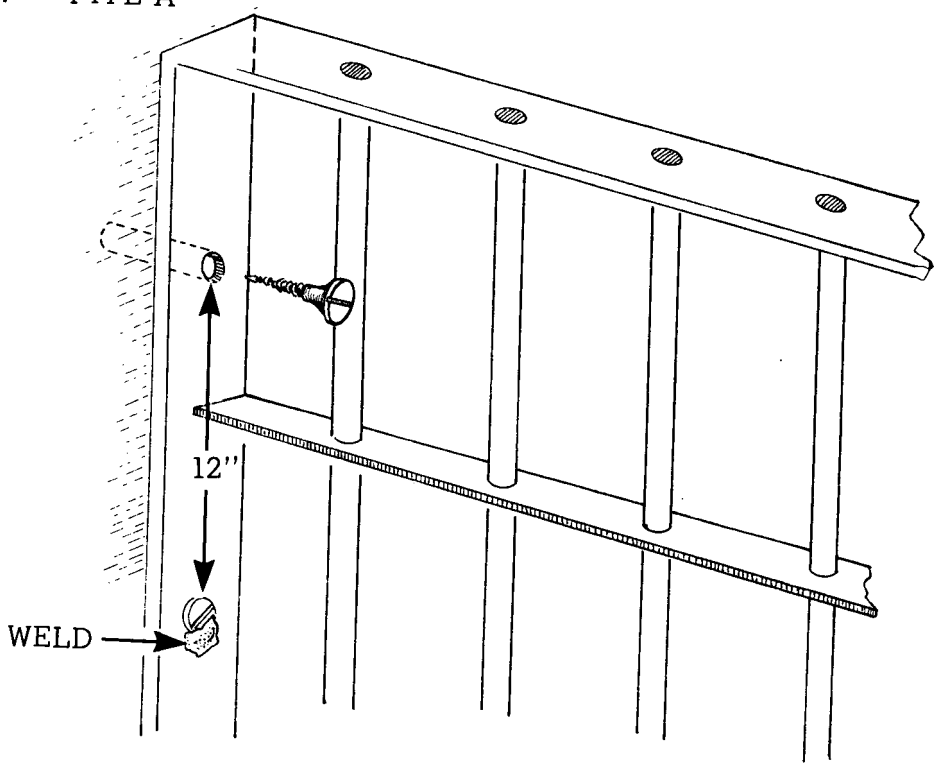
4. Because of the variety of ways that sound can be transmitted through a solid or semi-solid surface, it is impractical to attempt to provide construction standards that will guarantee satisfactory sound attenuation in all situations. If a problem exists or if new construction is

planned, the professional guidance of a qualified architect or sound engineer should be sought. If general background information is desired, it can be found in the sixth edition of Architectural Graphic Standards, published by John Wiley & Co., on pages 502 through 516.

ANNEX D

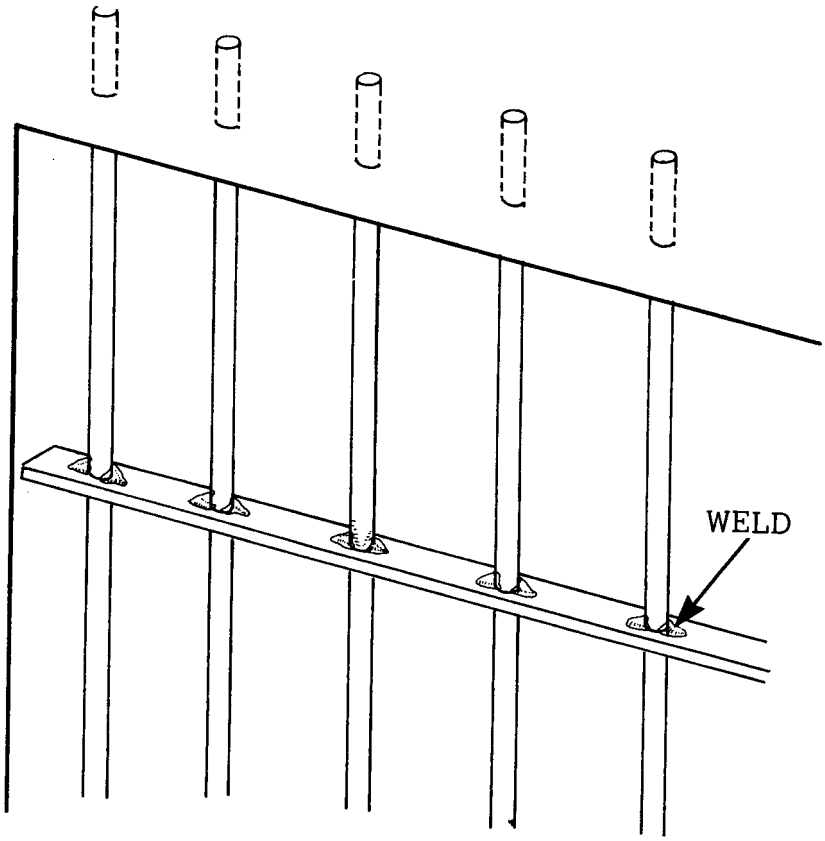
SPECIFICATIONS FOR BARRING WINDOWS

1. TYPE A



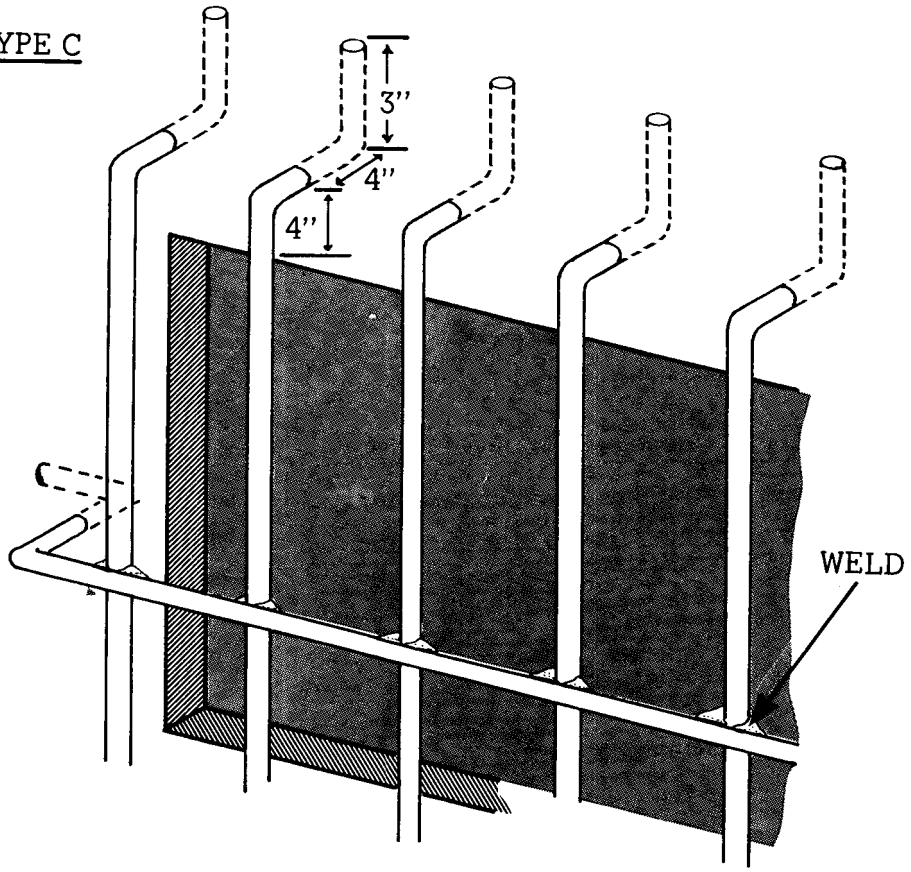
The steel frame must be a minimum of ⅜" thick by 3 inches wide. The steel bars must be a minimum of ½" in diameter and placed not more than 5 inches apart vertically. The horizontal steel supports must be a minimum of ¼" thick by 1½ inches wide and placed not more than 18 inches apart. The horizontal supports are to be drilled so that the vertical bars can be passed through them and be spot welded in place prior to installation. All joinings of frame, bars and supports, at top bottom or sides must be by welding. Frame must be held in masonry opening by using masonry anchors and steel screws that are not less than ⅜" in diameter by 3 inches long, with screw heads welded to frame. Screws and expanding anchors are to be located in the center of the frame width and placed every 12 inches around the entire frame; top, sides, and bottom.

2. TYPE B



Steel bars must be a minimum of ½" diameter and placed not more than 5 inches apart, vertically. Horizontal steel supports must be a minimum of ¼" thick by 1½ inches wide and placed not more than 18 inches apart. The horizontal supports are to be drilled so that the vertical bars can be passed through them and be spot welded in place prior to installation. The ends of each vertical bar will be embedded in the masonry a minimum depth of 3 inches. The entire bar work will be located back in the masonry opening at least 4 inches.

3. TYPE C



One-half inch diameter steel bars are used to form a grill work that is to be imbedded into the masonry wall around the window opening. Vertically the bars must be no more than 5 inches apart; horizontally, no more than 18 inches apart. Horizontally, bars must be welded to each vertical bar. The point where bar ends, both vertical and horizontal, enter the masonry must be a minimum of 4 inches from the edge of the opening. The angled bar ends should extend into the masonry a minimum of 4 inches, with the bent end being a minimum of 3 inches.

ANNEX E

MINIMUM SPECIFICATIONS FOR LOCALLY FABRICATED OR LOCALLY AVAILABLE MAIN ENTRANCE AND EMERGENCY EXIT DOORS

1. **Locally Available or Locally Fabricated Main-Entrance Doors:**

   a. Metal-clad type, minimum 16 gauge face, or

   b. Solid-wood door with a minimum thickness of 1¾ inches, and

   c. Both doors above shall be equipped with a pneumatic door closer and the following or equal: An approved Group 1 combination lock with an extension 50 and backed with appropriate drill-resistant ⅛" thick hard plate. Install the hard plate between the body of the lock and the interior side of the door. Weld all hinge pins, top and bottom, to their respective hinges when doors are installed with hinge pins located on the exterior face of the door. Otherwise, each hinge pin must be secured by a setscrew threaded through one point of the hinge pin proper. Position the setscrew to prevent access (or removal) of it when the door is closed.

2. Flat-sill fire doors having a half hour to one hour rating are authorized provided that the appropriate hard plate exists around the lock and that the door has an emergency escape device shield or a round door knob.

3. **Doors for Secure Working Areas and Continuous Operation Facilities:**

   a. Install a perimeter door having enough strength to prevent its being forcefully entered without leaving evidence of such entry.

   b. These doors above must be equipped with a pneumatic door closer and the following or equal: An approved Group 1 combination lock with an extension 50 and backed with appropriate drill-resistant ⅛" thick hard plate. Install the hard plate between the body of the lock and the interior side of the door. Weld all hinge pins, top and bottom, to their respective hinges when doors are installed with hinge pins located on the exterior face of the door. Otherwise, each hinge pin must be secured by a setscrew threaded through one point of the hinge pin proper. Position the setscrew to prevent access (or removal) of it when the door is closed.

4. **Access-Control Doors:** The use of a vault door for controlling access to a facility is not authorized as this type of continued use will create undue wear on the door and will eventually weaken the locking mechanism, cause malfunctioning of the emergency-escape device, and become a security and safety hazard. To preclude this install a second door for access during duty hours. Use the doors listed in 1a and 1b above for this purpose. Equip access-control doors with pneumatic door closers.

5. **Emergency Exits:** An emergency-exit door must provide protection equivalent to the door prescribed for the entrance of the facility. However, when a prescribed door cannot be obtained, a door constructed according to the specifications outlined in paragraph 6, this Annex, is acceptable as an emergency exit. Emergency exit doors may be modified as follows:

   a. "Panic hardware" may be substituted for the approved Group 1 combination lock providing that the door is equipped with metal brackets and a center-door-mounted,

removable metal bar which can be secured to the wall. The metal bar must be in place and appropriately secured during nonduty hours.

b. Approved emergency-exit control locks may be used instead of the "panic hardware" and metal bars or the Group 1 combination lock.

c. When an emergency-exit control lock is used to secure double emergency doors, the unused leaf must be deadbolted top and bottom from the inside. The movable leaf shall also be equipped with an astragal strip.

d. Vault doors, equipped with escape devices, do not require the modifications stated in paragraph 5a and 5b above.

6. **Locally Fabricated Steel Secondary or Emergency Exit Doors for Vaults and Secure Areas:**

a. The door will be a single steel panel not exceeding 4 feet in width or 8 feet in height. The minimum panel thickness should be ¼" for secure areas and ½" for vault areas.

b. The door frame is to be constructed of steel at least ⅛" thick for secure areas and ¼" thick for vault areas. The door stop must be continuously welded to the frame. It may be a solid block of metal (Detail B) or a "U" channel (Detail A); however the stop must extend out from the frame sufficiently to allow at least a one inch contact with the door panel at sides and top. The frame should extend over the wall, sides and top, a minimum of 4 inches.

c. Normally doors of this type must open outward for safety reasons and, therefore, the hinges are on the outside. Heavy duty steel hinges will be used, at least three per door panel. These hinges should be welded to the panel and frame, and the hinge pins welded to the butts.

d. Four steel bar holding brackets, at least 4 inches wide and ¼" thick, will be welded to the inside of the door in the approximate location shown on the attached drawing. The top two brackets are to be positioned approximately one third of the distance from the top to the bottom of the door, the bottom brackets two thirds of the same distance.

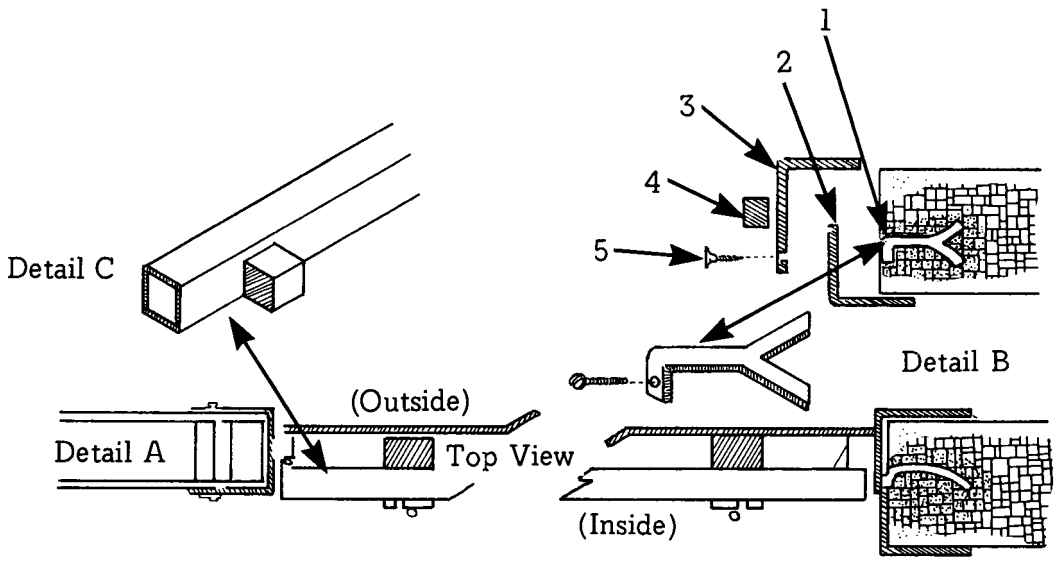
e. Two steel bars are to be made (Detail C) for placement in the brackets. The bars can be constructed of two steel angles or "U" channels welded together and, when completed, should be approximately 3 inches to 4 inches square. The length of the bars will be such that, when in place, they provide a close fit in the door jamb, overlapping the door stop/mullion by 1 inch or more.

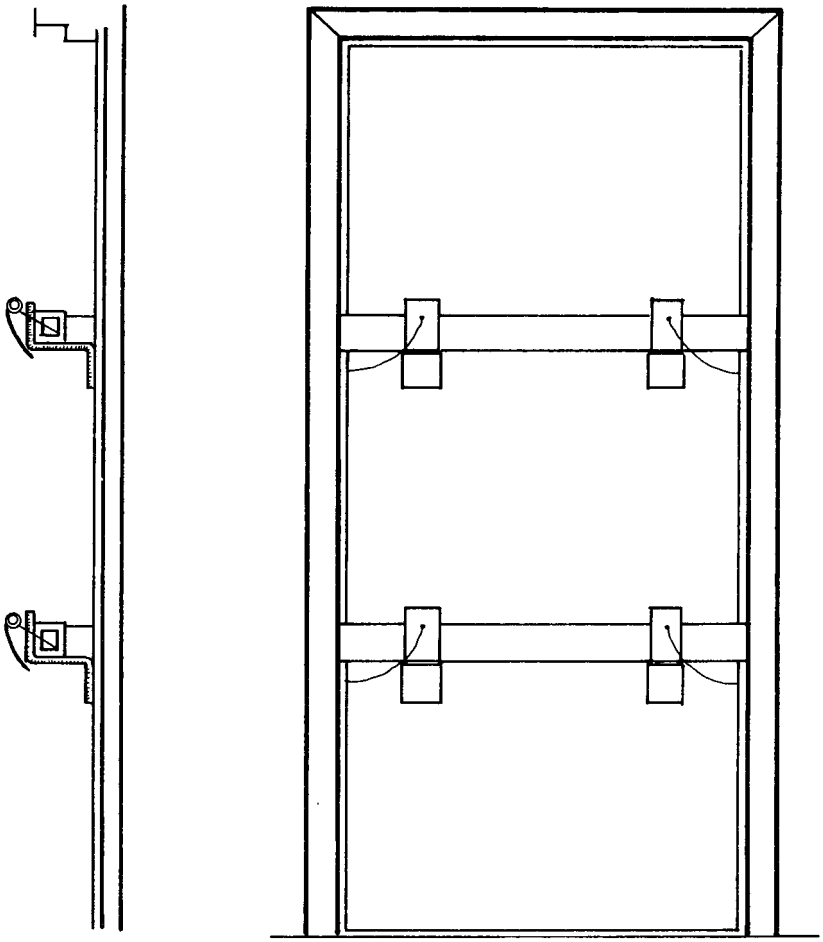
f. The bars and brackets are to be drilled at a downward angle to accommodate ¼" steel pins. The pins are to be sufficiently long to bottom out in the inside of the bars and are to be secured with chains welded or otherwise attached to the door jamb; attachment is to keep the pins from being lost. The fit of the pins must permit ready removal by hand.

g. Spacer blocks are to be provided with each of the bar and bracket units. These blocks serve to cause a proper, snug fit of the bars when in place. The blocks may be of either steel or wood. If steel, they may be welded to the bars; if wood, they may be drilled and attached with bolts.

h. Detail A depicts a means of securing a door frame to a light secure area type wall, such as wood studs and dry wall reinforced with steel or expanded metal. A "U" channel or two angles are adjusted and welded together to form the frame around the wall opening. It is then bolted in place by the use of carriage bolts having their rivet-like heads on the outside and the nut on the inside. The bolts at the nut end will be peened over or spot welded to preclude tampering. The bolts should be at least ⅜" in diameter and installed so that their heads fit tight and flush against the outside of the frame. Bolts will be installed in both sides and top of the frame and spaced approximately 18 inches apart.

i. Detail B depicts a suggested method for installing a frame in a masonry wall. Pieces of steel 1½ inches to 2 inches wide by ¼" thick are formed as shown and grouted into the masonry of the door opening every 12 inches to 18 inches at both sides and top. The hole in the end, kept flush with the opening, will be drilled and tapped to receive the screw selected. This screw should be of steel, ⅜" or more in diameter, and will be long enough to extend through all three pieces of metal. Two angles, as shown in the detail, are then put in place and screwed together. The door stop, be it a solid block or "U" channel, is then continuously welded in place on both sides and top of the frame. This method of installing a steel door frame is extremely effective from the standpoint of strength. If the steel piece is not used, a ⅜" diameter steel lag bolt, shaped in an L, may be grouted into the masonry with its threaded end out. The two angles are then installed with holes to permit the threaded end to protrude through them and a nut is used to bolt the frame in place. This method is as effective, but is more unsightly and personnel passing through the door are apt to catch clothing on the protruding bolt ends.





Side View

View of inside Door

ANNEX F

TECHNICAL SECURITY

1. **TECHNICAL SURVEILLANCE COUNTERMEASURES:** TSCM inspections and surveys will be conducted as specified by cognizant SIOs for the SCIFs involved.
2. **COMPUTER SECURITY:** All automatic data-processing equipment used to handle or store SCI will be operated in compliance with DCID 1/16 (Security of Foreign Intelligence in Automated Data Processing Systems and Networks).
3. **COMPROMISING EMANATIONS CONTROL:** All equipment used to transmit or process SCI electronically, including communications, word-processing, and automatic data-processing systems and equipment, must satisfy the requirements of USCSB 4-11 (National Policy on Control of Compromising Emanations). (See appendix D.) All compromising emanations must be contained within boundaries specified by the TEMPEST accreditation authority.
4. **PERSONAL EQUIPMENT:** Personally owned electronic equipment shall not be introduced into an SCIF.