



Change One to Annex B incorporated on 9 December 2004



JOINT
AIR FORCE - ARMY - NAVY

JAFAN 6/9

Manual

Physical Security Standards
for Special Access Program Facilities

23 March 2004



TABLE OF CONTENTS

FOREWORD.....	3
1. POLICY AND CONCEPT.....	4
1.1 Policy Statement.....	4
1.2 Concept.....	4
1.3 American Disabilities Act (ADA) Review.....	4
2. GENERAL ADMINISTRATIVE.....	5
2.1 SAP Facilities (SAPFs).....	5
2.2 Physical Security Preconstruction Review and Approval.....	5
2.3 Accreditation.....	5
2.4 Co-Utilization.....	6
2.5 Personnel Controls.....	6
2.6 Control of Combinations.....	6
2.7 Entry/Exit Inspections.....	6
2.8 Control of Electronic Devices and Other Items.....	6
3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SAPFs.....	7
3.1 Construction Policy for SAP Facilities.....	7
3.2 Temporary Secure Working Area (TSWA).....	8
3.3 Requirements Common To All SAPFs; Within The US and Overseas.....	9
4. CONSTRUCTION SPECIFICATIONS.....	10
4.1 Vault Construction Criteria.....	10
4.2 SAPF Criteria When Using Permanent Dry Wall Construction.....	11
4.3 SAPF Construction Criteria When Using Steel Plate.....	11
4.4 SAPF Construction Criteria When Using Expanded Metal.....	11
4.5 General.....	11
5. GLOSSARY.....	11
ANNEX A - SAPF Accreditation Checklist.....	14
ANNEX B - Intrusion Detection Systems (IDS).....	33
ANNEX C - Acoustical Control and Sound Masking Techniques.....	41
ANNEX D - Personnel Access Controls.....	43
ANNEX E - Telecommunications Systems and Equipment.....	45



FOREWORD

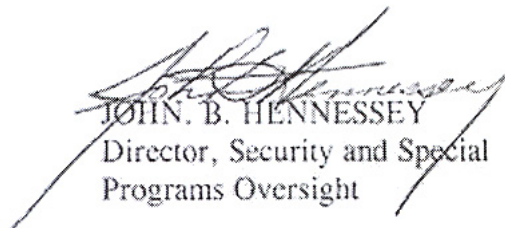
This Manual provides enhanced Physical Security Standards for Special Access Program Facilities (SAPFs) supporting Air Force, Army and Navy DoD SAPs and SAP-type compartmented efforts established and approved by the Executive Branch.

The Director of Central Intelligence Directive (DCID) 6/9 of 18 November 2002 was used as the model publication from which this Manual was crafted. The subject matter and order of presentation closely resemble DCID 6/9. No specific security measure contained in this Manual exceeds the requirements for physical security standards supporting Sensitive Compartmented Information (SCI) facilities.

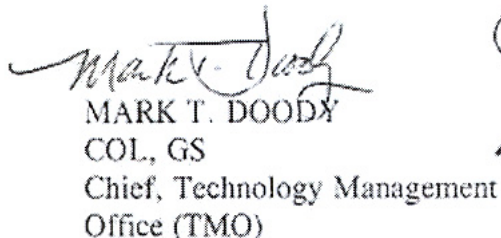
Throughout this Manual it is understood that whenever a security alternative is specified for a SAP by the government Program Security Officer (PSO), his or her authority is strictly based on the security determinations of the service component Cognizant Security Authority/Agency (CSA). CSA is defined as Authorities/Agencies of the Department of Defense (DoD) military departments that have been delegated the responsibility authorized by E.O. 12829 to establish an industrial security program for the purpose of safeguarding classified information under the jurisdiction of each military department when disclosed or released to U.S. Industry. This authority is complemented by the National Industrial Security Program Operating Manual (NISPOM) and the DoD Overprint to the NISPOM Supplement, and for the purposes of this directive specifically refers to the DoD military department Special Access Program (SAP) activities authorized by E.O. 12958 employing enhanced security measures exceeding those normally required by DoD 5200.1-R for information at the same classification level. DoD SAP CSAs are the DoD military department Special Access Programs Coordinators (SAPCOs).

The provisions of this Manual are applicable to all government and contractor personnel participating in the administration of DoD SAPs. In cases of doubt over the requirements of this Manual, users should consult the PSO prior to taking any action or expending program-related funds. In cases of extreme emergency requiring immediate attention, the action taken should protect the Government's interest and the security of the program from compromise.

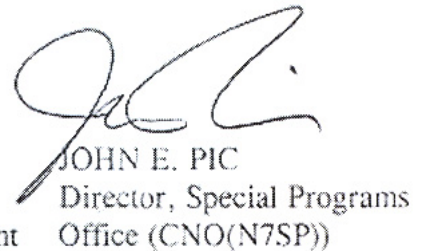
This Manual is intended to be a living document. Users are encouraged to submit change recommendations to service component SAPCOs via their cognizant security office.


JOHN B. HENNESSEY
Director, Security and Special
Programs Oversight

USAF


MARK T. DOODY
COL, GS
Chief, Technology Management
Office (TMO)

USA


JOHN E. PIC
Director, Special Programs
Office (CNO(N7SP))

USN



1. POLICY AND CONCEPT

1.1 Policy Statement

1.1.1 Physical security standards are hereby established governing the construction and protection of facilities for storing, processing, and discussion of Special Access Program (SAP) information which requires extraordinary security safeguards. Compliance with this Joint Air Force-Army-Navy Implementation Manual (hereafter referred to as the "Manual") is mandatory for all Special Access Program Facilities (SAPFs) established after the effective date of this manual, including those that make substantial renovations to existing SAPFs. Those SAPFs approved prior to the effective date of this Manual will not require modification to meet these standards; however, documentation approved by the PSO must be maintained on file within the SAPF indicating that the physical security construction of the facility occurred prior to the effective date of this Manual.

1.1.2 The physical security safeguards set forth in this Manual are the standards for the protection of SAP information within the Departments of the Air Force, Army and Navy. Only the Component Level SAP Central Office may impose more stringent standards if they believe extraordinary conditions and circumstances warrant. This authority may only be delegated by the Service Component SAPCO. Additional cost resulting from more stringent standards should be borne by the requiring Agency, Department, or relevant contract.

1.1.3 In situations where conditions or unforeseen factors render full compliance to these standards unreasonable, security officers in the grade of GS-14 or O-5 or above may apply commensurate levels of protection to specific requirements within this Manual. Commensurate levels of protection will not be designed with the intent to reduce or lessen the security protection of the area of consideration. Any waivers to the specific requirements of this Manual must be approved in writing by the Service Component SAPCO or delegated representative.

1.1.4 All SAPFs must be formally accredited in writing by a government PSO or designee prior to conducting any SAP activities.

1.1.5 A single person is now authorized to staff a SAPF, eliminating the requirement for the two-person rule concept. The elimination of the two-person concept applies only to the staffing level of a

facility vice the transmission requirements of classified material outlined in the DoD Overprint to the NISPOMSUP.

1.2 Concept

1.2.1 SAPF design must balance threats and vulnerabilities against appropriate security measures in order to reach an acceptable level of risk. Each security concept or plan must be submitted to the PSO for approval. For the purposes of this Manual, the PSO is defined as the accreditation authority for the compartmented facility. Protection against surreptitious entry, regardless of SAPF location, is always required. Security measures must be taken to deter technical surveillance of activities taking place within the SAPF. TEMPEST security measures must be considered if electronic processing of SAP information is involved.

1.2.2 On military and civilian compounds, security controls may exist such as identification checks, perimeter fences, police patrols, and other security measures which form a basis for what is considered "security-in-depth." Security in-depth is considered when supplemental protection is afforded together with the SAPF location whereas internal security systems may be sufficient to be used in lieu of certain physical security or construction requirements contained in this Manual.

1.2.3 Proper security planning for a SAPF is intended to deny foreign intelligence services and other unauthorized personnel the opportunity for undetected entry into those facilities and exploitation of sensitive activities. Faulty security planning and equipment installation not only jeopardizes security but wastes money and resources. Adding redundant security features causes extra expense which could be used on other needed features. When security features are neglected during initial construction, retrofitting of existing facilities to comply with security requirements becomes necessary and extremely costly.

1.3 American Disabilities Act (ADA) Review

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



2. GENERAL ADMINISTRATIVE

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

2.2 Physical Security Preconstruction Review and Approval. PSOs shall review physical security preconstruction plans for SAPF construction, expansion or modification. All documentation pertaining to SAPF construction will be restricted and released on an as-needed basis. The approval or disapproval of a physical security preconstruction plan shall be made a matter of record.

2.2.1 The requester shall submit a Fixed Facility Checklist (FFC, Annex A) to the respective PSO for review and approval. The completed Fixed Facility Checklist will be classified in accordance with specific Program security classification guidance.

2.2.2 The Checklist submission shall include floor plans, diagrams of electrical communications wiring, heating, ventilation, air conditioning (HVAC) connections, security equipment layout (to include the location of intrusion detection equipment), etc. All diagrams or drawings must be submitted on legible and reproducible media.

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

2.3 Accreditation. The PSO will ensure SAPFs comply with JAFAN 6/9. The PSO is authorized to inspect any SAPF, direct action to correct any deficient situation, and withdraw SAPF accreditation. The procedures for establishment and accreditation of SAPFs are prescribed below:

2.3.1 The procedures for establishment and accreditation of a SAPF from conception through construction must be coordinated and approved by the PSO.

2.3.2 SAP information shall never be handled, processed, discussed, or stored in any facility other than a properly accredited SAPF unless written authorization is granted by the PSO.

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

- JAFAN 6/9 Fixed Facility Checklist.
- Accreditation authorization documents (e.g., physical, TEMPEST, and AIS).
- Inspection reports, including TSCM reports, for the entire period of SAPF accreditation.
- Operating procedures, Command/Contractor Program Security Officer (CPSO) appointment letters, Memoranda of Agreement (MOAs), Emergency Action Plans, etc.
- Copies of any waivers granted by the PSO.

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

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

2.3.5.1 Facilities undergoing major modification may be required to comply entirely with the provisions of this Manual. Approval for such modifications shall be requested through the PSO and



received prior to any modifications taking place within the SAPF.

2.3.5.2 In the event a need arises to reaccredit a SAPF after the accreditation has been terminated, the PSO may approve the use of a previously accredited SAPF in accordance with paragraph 5-806 of the DoD Overprint to the NISPOMSUP.

2.3.6 Withdrawal of Accreditation

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

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

2.4 Co-Utilization

2.4.1 Agencies desiring to co-utilize a SAPF may accept the current accreditation of the cognizant agency. Prospective tenant activities will be informed of all exceptions, conditions and/or waivers to the requirements of this manual prior to co-utilization. Any security enhancements required by an agency or department requesting co-utilization should be funded by that organization, and must be approved by the appropriate Service SAPCO prior to implementation. A co-utilization agreement must be established prior to occupancy.

2.4.2 The co-location/co-utilization of Sensitive Compartmented Information within a SAPF will require authorization from the facility PSO.

2.5 Personnel Controls

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

2.6 Control of Combinations

2.6.1 Combinations to locks will not be the same throughout a SAPF, e.g. doors, vaults, etc. Combinations to locks installed on security containers/safes, perimeter doors, windows and any other openings should be changed immediately whenever:

- A combination lock is first installed or used;
- A combination has been subjected, or believed to have been subjected to compromise;
- Whenever an individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock; and
- At other times when considered necessary by the PSO.

2.6.2 All combinations to SAPF entrance doors may be stored in another SAPF of equal or higher accreditation level, or when not feasible, alternate arrangements can be made in coordination with the PSO.

2.7 Entry/Exit Inspections. The SAPF will have procedures prescribed for inspecting personal belongings and vehicles at the entry or exit points of SAPFs, or at other designated points of entry to the building, facility, or compound. The purpose of the inspection is to deter the unauthorized removal of classified material, and deter the introduction of prohibited items or contraband. This shall include determination of whether inspections are randomly conducted or mandatory for all, and whether they apply for visitors only or for the entire staff assigned. All personnel inspection procedures should be reviewed by the facility's legal counsel prior to promulgation.

2.8 Control of Electronic Devices and Other Items

2.8.1 The PSO shall ensure that procedures are instituted for control of electronic devices and other items introduced into or removed from the SAPF. Specific guidance concerning Automated Information System(s) is provided in DCID 6/3. It is the policy of Service Component SAPCOs that electronic equipment will not be routinely carried into or out of SAPFs. Electronic equipment may be allowed into a SAPF in accordance with supplemental direction provided by component SAPCOs.

2.8.2 The prohibition against electronic equipment in SAPFs does not apply to those needed by the disabled or for medical or health reasons (e.g.



motorized wheelchairs, hearing aids, heart pacemakers, amplified telephone headsets, teletypewriters for the hearing impaired). However, the PSO or CPSO when approved by the PSO shall establish procedures within the Facility SOP for notification that such equipment is being entered in to the SAPF.

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

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

3. PHYSICAL SECURITY CONSTRUCTION POLICY FOR SAPFs

3.1 Construction Policy for SAP Facilities. Physical security criteria is governed by whether the SAPF is located in the US or not, according to the following conditions: closed storage, open storage, continuous operations, secure working areas.

3.1.1 Closed Storage

3.1.1.1 Inside US

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

3.1.1.2 Outside US

- The SAPF must meet the construction specifications for SAPFs as set forth in Chapter 4 (Steel Plate or Expanded Metal). SAPFs within US Government controlled compounds¹, or equivalent, having armed immediate response forces may use specifications indicated in Chapter 4 (Permanent Dry Wall Construction) with prior approval of the PSO.
- The SAPF must be alarmed in accordance with Annex B.
- SAP information must be stored in GSA-approved containers having a rating for both forced and surreptitious entry.
- There must be a response force capable of responding to an alarm within 10 minutes and a reserve response force available to assist the responding force.

3.1.2 Open Storage

3.1.2.1 Inside US: When open storage is justified and approved by the PSO, the SAPF must:

- be alarmed in accordance with Annex B;
- have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the response force;
- use specifications indicated in Chapter 4 (Permanent Dry Wall Construction); and
- the PSO may require any SAPF perimeter walls accessible from exterior building ground level to meet the equivalent protection afforded by Chapter 4 (Expanded Metal) construction.

3.1.2.2 Outside US: Open storage of SAP material will be avoided. When open storage is justified as mission essential and approved by the PSO, vault construction is preferred. The SAPF must:

- be alarmed in accordance with Annex B;
- have a response force capable of responding to an alarm within 5 minutes and a reserve response force available to assist the responding force;
- have an adequate, tested plan to protect, evacuate, or destroy the material in the event of emergency or natural disaster; and

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



- meet one of the following:
 - The construction specification for vaults set forth in Chapter 4 (Vaults); or
 - With the approval of the PSO, SAPFs located on a controlled US government compound may use expanded metal, steel plate, or GSA-approved modular vaults in lieu of vault construction.

3.1.3 Continuous Operation

3.1.3.1 Inside US

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

3.1.3.2 Outside US

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

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

3.1.4.1 Inside US

- The Secure Working Area SAPF must meet the specifications set forth in Chapter 4 (Permanent Dry Wall Construction).
- The Secure Working Area SAPF must be alarmed with a balanced magnetic switch on all perimeter entrance doors.
- No storage of SAP material is authorized.
- There must be a response force capable of responding to an alarm within 15 minutes after annunciation, and a reserve response force available to assist the responding force.

3.1.4.2 Outside US

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

3.2 Temporary Secure Working Area (TSWA)

3.2.1 A Temporary Secure Working area is defined as a temporarily accredited facility that is used no more than an average of 40 hours per month over a 12 month period, for the handling, discussion, and/or processing of SAP information, however, SAP material shall not be stored within the TSWA.

3.2.2 During the entire period the TSWA is in use, the entrance will be controlled and access limited to persons having the appropriate level of clearance, access and a validated need-to-know for which the area has been approved. Approval for using such areas must be obtained from the PSO setting forth room number(s), building, location, purpose, and specific security measures employed during usage as well as during other periods. No special construction is required other than to meet sound attenuation requirements as set forth in Annex D, when applicable. If such a facility must also be used for the discussion of SAP information, a Technical



Surveillance Countermeasures (TSCM) evaluation may be required at the discretion of the PSO, as conditions warrant.

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

- Maintained at a US Secret level.
- Secured with a keylock or a combination lock approved by the PSO.
- Access will be limited to personnel possessing a US Secret clearance.

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

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

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

3.3.2 Sound Attenuation: The SAPF perimeter walls, doors, windows, floors and ceiling, including all openings, shall provide sufficient sound attenuation to preclude inadvertent disclosure of conversation. The requirements for sound attenuation are contained within Annex D.

3.3.3 Entrance, Exit, and Access Doors

3.3.3.1 Primary entrance doors to SAPFs shall be limited to one. If circumstances require more than one entrance door, approval must be obtained from the PSO. In most circumstances, an emergency exit door is required. In cases where local fire codes conflict with security practices, the issue of life and safety shall take precedence over security directives and must be complied with provided the PSO has determined the conflict is within an acceptable managed risk. All instances of this nature will be fully documented and retained on file with the accreditation documentation for the facility. All perimeter SAPF doors must remain closed when not in use, with the exception of emergency circumstances. If a door must be left open, access will be controlled by a Program briefed on-site person.

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

3.3.3.3 All SAPF primary entrance doors must be equipped with an automatic door closer, a GSA-approved combination lock meeting Federal Specification FF-L-2740A and an access control device with the following requirements:²

- If doors are equipped with hinge pins located on the exterior side of the door where it opens into an uncontrolled area outside the SAPF, the hinge pins will be spot welded or have set screws installed to prevent removal of the door.
- If a SAPF entrance door is not used as an access control door and stands open in an uncontrolled area, the combination lock will be protected against unauthorized access/tampering. The method used for the protection of the locking mechanism will be approved by the PSO.

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

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

3.3.3.6 Door Construction Types: Selections of entrance and emergency exit doors shall be consistent with SAPF perimeter wall construction. Some acceptable types of doors include:

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



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

3.3.4 Physical Protection of Vents, Ducts and Pipes

3.3.4.1 All vents, ducts, and similar openings in excess of 96 square inches that enter or pass through a SAPF must be protected with either steel bars or grills. In addition, duct sound baffles that meet appropriate sound attenuation class (Group 3) as specified in Annex D will be used. Within the United States, bars or grills are not required if an IDS is used. If one dimension of the duct measures less than six inches, or duct is less than 96 square inches, bars or grills are not required; however, all ducts must be treated to provide sufficient sound attenuation. If bars are used, they must be 1/2 inch diameter steel spot welded to the steel structure; if commercial sound baffles are used, the baffles or wave forms must be metal permanently installed and no farther apart than six (6) inches in one dimension. A deviation of 1/2 inch in vertical and/or horizontal spacing is permissible.

3.3.4.2 Based on the TEMPEST accreditation, it may be required that all vents, ducts, and pipes must have a non-conductive section (a piece of dissimilar material e.g., canvas, rubber) which is unable to carry an electromagnetic current beyond the perimeter of the SAPF. All physical security protective features will be installed within the boundary perimeter of the SAPF.

3.3.4.3 An access port to allow visual inspection of the protection in the vent or duct should be installed inside the secure perimeter of the SAPF. If the inspection port must be installed outside the perimeter of the SAPF, it must be controlled by a key locking mechanism.

3.3.5 Windows

3.3.5.1 All windows which might reasonably afford visual surveillance of personnel, documents,

materials, or activities within the facility, shall be made opaque or equipped with blinds, drapes or other coverings to preclude such visual surveillance.

3.3.5.2 Windows at ground level³ will be constructed from or covered with materials that will provide protection from forced entry. The protection provided to the windows need be no stronger than the strength of the contiguous walls. Windows are to be made inoperable by either permanently sealing them or equipping them on the inside with a locking mechanism.

3.3.5.3 All perimeter windows at ground level shall be protected with an approved IDS. (Annex B).

4. CONSTRUCTION SPECIFICATIONS

4.1 Vault Construction Criteria

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

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

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

³ 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., electrical transformer, air conditioning units, vegetation or landscaping which can easily be climbed, etc.).



reinforced concrete, a steel liner is to be constructed the same as the walls to form the floor and ceiling of the vault. Seams where the steel plates meet horizontally and vertically are to be continuously welded together.

4.1.4 All vaults shall be equipped with a GSA-approved Class 5 or Class 8 vault door. Within the US, a Class 6 vault door is acceptable.

4.2 SAPF Criteria When Using Permanent Dry Wall Construction. Walls, floor and ceiling will be permanently constructed and attached to each other. To provide visual evidence of attempted entry, all construction, to include above the false ceiling and below a raised floor, must be done in such a manner as to provide visual evidence of unauthorized Penetration.

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

4.4 SAPF Construction Criteria When Using Expanded Metal. Walls are to be reinforced, slab-to-slab, with a minimum of 9-gauge expanded metal.

4.5 General

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

5. GLOSSARY

Access Control System: A system to identify and/or admit personnel with properly authorized access to a SAPF using physical, electronic, and/or human controls.

Accreditation: The formal approval of a specific place, referred to as a Special Access Program

Facility (SAPF), that meets prescribed physical, technical, and personnel security standards.

Acoustic Security: Those security measures designed and used to deny aural access to classified information.

Astragal Strip: A narrow strip of material applied over the gap between a pair of doors for protection from unauthorized entry and sound attenuation.

Authorized Personnel: A person who has been granted access to the SAPF based upon the requisite clearance, access and valid need to know as determined by the PSO.

Balanced Magnetic Switch (BMS): A type of IDS sensor which may be installed on any rigid, operable opening (i.e., doors, windows) through which access may be gained to the SAPF.

Break-Wire Detector: An IDS sensor used with screens and grids, open wiring, and grooved stripping in various arrays and configurations necessary to detect surreptitious and forcible penetrations of movable openings, floors, walls, ceilings, and skylights.

Closed Storage: The storage of SAP material in properly secured GSA-approved security containers within an accredited SAPF.

Computerized Telephone System (CTS): Also referred to as a hybrid key system, business communication system, or office communications system.

Cognizant Security Authority/Agency (CSA): The single principal designated by the SAP Service Component to serve as the responsible official for administering all aspects of SAP program security. DoD SAP CSAs are the DoD military department Special Access Programs Coordinators (SAPCOs).

Continuous Operation: This condition exists when a SAPF is staffed 24 hours every day.

Controlled Area/Compound: Any area to which entry is subject to restrictions or control for security reasons.

Controlled Building: A building to which entry is subject to restrictions or control for security reasons.

Co-Utilization: Two or more organizations sharing the same SAPF.



Dead Bolt: A lock bolt with no spring action. Activated by a key or turn knob and cannot be moved by end pressure.

Deadlocking Panic Hardware: A panic hardware with a deadlocking latch that has a device when in the closed position resists the latch from being retracted.

Decibel (db): A unit of sound measurement.

Document: Any recorded information regardless of its physical form or characteristics, including, without limitation, written or printed matter, data processing cards and tapes, maps, charts, paintings, drawings, photos, engravings, sketches, working notes and papers, reproductions of such things by any means or process, and sound, voice, magnetic or electronic recordings in any form.

Dual Technology: PIR, microwave or ultrasonic IDS sensors which combine the features of more than one volumetric technology.

Expanded Steel: Also called EXPANDED METAL MESH. A lace work patterned material produced from 9/11 gauge sheet steel by making regular uniform cuts and then pulling it apart with uniform pressure.

Guard: A properly trained and equipped individual whose duties include the protection of a SAPF. Guards will be US citizens and with primary duty focus on the protection of US Government classified information. Guards will possess a US SECRET clearance.

Intelligence Community (and agencies within the Community): Refers to the United States Government agencies and organizations identified in section 3.4(f) (1 through 7) of Executive Order 12333.

Intrusion Detection System: A security alarm system to detect unauthorized entry.

Isolator: A device or assembly of devices which isolates or disconnects a telephone or Computerized Telephone System (CTS) from all wires which exit the SAPF and which has been accepted as effective for security purposes by the Telephone Security Group (TSG approved).

Key Service Unit (KSU): An electromechanical switching device which controls routing and operation of an analog telephone system.

Line Supervision:

Class I: Class I line security is achieved through the use of DES or an algorithm based on the cypher feedback or cypher block chaining mode of encryption. Certification by NIST or another independent testing laboratory is required.

Class II: Class II line supervision refers to systems in which the transmission is based on pseudo random generated or digital encoding using an interrogation and response scheme throughout the entire communication, or UL Class AA line supervision. The signal shall not repeat itself within a minimum six month period, Class II security shall be impervious to compromise using resistance, voltage, current, or signal substitution techniques.

Motion Detection Sensor: An alarm sensor that detects movement.

Non-Conductive Section: Material (i.e. canvas, rubber, etc.) installed in ducts, vents, or pipes, and is unable to carry audio or radio frequency (RF) emanations.

Non-Discussion Area: A clearly defined area within a SAPF where classified discussions are not authorized due to inadequate sound attenuation.

Open Storage: The storage of SAP material within a SAPF in any configuration other than within GSA-approved security containers.

Response Force: Personnel (not including those on fixed security posts) appropriately equipped and trained, whose duties include initial or follow up response to situations which threaten the security of the SAPF. This includes local law enforcement support or other external forces as noted in agreements.

Secure Working Area: An accredited SAPF used for handling, discussing and/or processing of SAP information, but where SAP material will not be stored.

Security In-Depth: A determination made by the PSO that a facility's security program consists of layered and complementary security controls



sufficient to deter and detect unauthorized entry and movement within the facility.

Sensitive Compartmented Information (SCI): SCI is classified information concerning or derived from intelligence sources, methods or analytical processes, which is required to be handled exclusively within formal control systems established by the Director of Central Intelligence.

Sensitive Compartmented Information Facility (SCIF): An accredited area, room, group of rooms, building, or installation where SCI may be stored, used, discussed and/or electronically processed.

Sound Group: Voice transmission attenuation groups established to satisfy acoustical requirements. Ratings measured in sound transmission class may be found in the Architectural Graphic Standards.

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

Special Access Program (SAP): Any approved program which imposes strict clearance and investigative criteria, need-to-know and access controls beyond those normally required for access to CONFIDENTIAL, SECRET, or TOP SECRET information.

Special Access Program Facility (SAPF): An accredited area, room, group of rooms, building, or installation where SAP information/material may be stored, used, discussed and/or electronically processed.

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

Tactical SAPF (T-SAPF): An accredited area used for actual or simulated war operations for a specified period of time.

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

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

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

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



(Classify and date appropriately when filled in)

JOINT AIR FORCE – ARMY – NAVY (JAFAN) 6/9
ANNEX A
SAPF FIXED FACILITY ACCREDITATION CHECKLIST

Effective Date:

Check One

- Pre-construction New Facility Modified Facility Page Change

Checklist Contents

Section A	General Information	2
Section B	Peripheral Security	5
Section C	SAPF Security	6
Section D	Doors	8
Section E	Intrusion Detection Systems (IDS)	9
Section F	Telecommunication Systems and Equipment Baseline	13
Section G	Acoustical Protection	17
Section H	Classified Destruction Methods	18
Section I	TEMPEST / Technical Security	19

Classification



Section A – General Information

1. SAPF Data:

Organization/Company Name: _____

SAPF Identification Number (If applicable): _____

Organization subordinate to (If applicable): _____

Contract Number & Expiration Date (If applicable): _____

Concept Approval Date: _____ by: _____

Program Security Officer (PSO): _____

Defense Special Security Communication System (DSSCS) Information [If applicable]

DSSCS Message Address: _____

DSSCS INFO Address: _____

If no DSSCS Message Address, please provide passing instructions: _____

2. SAPF Location:

Street Address:

Bldg Name/#: _____ Floor(s): _____

Suite(s): _____ Room(s) #: _____

City: _____ Base/Post: _____

State/Country: _____ ZIP Code: _____

3. Mailing Address (if different from SAPF location):

Street or P.O. Box: _____

City: _____ State: _____ Zip Code: _____

Classification



4. E-Mail Address:

(Classified) _____ (Network/System Name & Level) _____

(Unclassified) _____ (Network/System Name) _____

(Other) _____ (Network/System Name) _____

5. Responsible Security Personnel:

Primary Name: _____ Alternate Name: _____

Commercial Telephone: (Primary) _____ (Alternate) _____

DSN Telephone: (Primary) _____ (Alternate) _____

Secure Telephone: (Primary) _____ (Alternate) _____

STU/STE Telephone: (Primary) _____ (Alternate) _____

Other Telephone: (Primary) _____ (Alternate) _____

Home Telephone: (Optional) _____

Fax No: (Classified) _____ (Unclassified) _____

Command or Regional Special Security office/name (SSO): *(If applicable)* _____

Commercial Telephone: (Primary) _____ (Alternate) _____

Other Telephone: (Primary) _____ (Alternate) _____

Information System Security Officer Name: _____

(Alternate Name): _____

Commercial Telephone: (Primary) _____ (Alternate) _____

Secure Telephone: (Primary) _____ (Alternate) _____

6. Accreditation Data:

a. Category/Compartments of SAP Requested: _____

1) Indicate storage requirement: Open Closed Continuous Operation None

2) Indicate the facility type: Permanent Semi-Permanent Secure Working Area

Temporary Secure Working Area Tactical

Classification



b. Existing Accreditation Information (If applicable):

1) Category/Compartments of SAP: _____

2) Accreditation granted by: _____ on _____

3) Storage exception: (i.e. fixed media) _____

c. SCI co-located within SAPF? YES NO. If Yes, identify SCI Classification Level (check all that apply): SAP Top Secret Secret Confidential

d. SAPF Duty Hours: _____ (hours to hours), _____ days per week.

e. Total square footage that the SAPF occupies: _____

f. Has PSO issued any Waivers? YES NO N/A (If YES, Attach copy of the Waiver)

7. Construction/modification:

Is construction or modification complete? YES NO N/A If NO, enter the expected date of completion: _____

8. Inspections:

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

b. Were deficiencies corrected? YES NO N/A If NO, explain: _____

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

Were deficiencies corrected? YES NO N/A If NO, explain: _____

d. Last Staff Assistance Visit by: _____ on: _____

9. Remarks: _____

Classification



Section B – Peripheral Security

1. Describe building exterior security:

- a. Is building located on a controlled compound: YES NO
- b. Fence Type: _____ Height: _____ Length: _____
- c. Fence Alarm: _____
- d. Fence lighting: _____
- e. Building lighting: _____
- f. Cameras/Television (CCTV)(include monitor location): _____
- g. Guards YES NO. If Yes, what kind of patrols are they? STATIC ROVING. Clearance Level of Guards, (If Applicable): _____, During what hours/days: _____, Any SAPF related duties? YES NO. If yes, describe duties: _____
- Comment: _____

2. Building: (Please provide legible general floor plan of SAPF perimeter on a 8.5" X 11" or 11" x 17" format)

- a. Construction type: _____
- b. Windows: _____
- c. Doors: _____
- d. Describe Access Controls: _____
Continuous: YES NO. If NO, during what hours? _____
- e. Interior Building Guards: YES NO. If YES, what type of patrols are they? STATIC ROVING. Clearance Level of Guards, (If Applicable): _____
During what hours/days: _____
- f. Building Alarmed (not SAPF): YES NO
If YES, Describe monitoring and response procedures? _____

3. Security In-Depth:

What external security attributes and/or features should the PSO consider for determining whether or not this facility has Security In-Depth? Please identify/explain all factors: _____

Classification



Section C – SAPF Security

1. How is access to the SAPF controlled?

a. By Guard Force: YES NO

If YES, what is their minimum Security Clearance Level: _____

b. By Assigned Personnel: YES NO

If YES, do personnel have visual control of SAPF entrance door? YES NO N/A

c. By Access Control Device: YES NO

If YES, what kind? Automated Access Control System Non-Automated.

If non-Automated:

1) Is there a by-pass key? YES NO N/A

If YES, how is the by-pass key protected? _____

2) Manufacturer: _____ Model: _____

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

If Automated:

1) Are access Control Transmission lines protected by 128-bit encryption: YES NO
If NO, explain the physical protection provided? _____

2) Are Automated Access Control system locations within a SAPF or an alarmed area controlled at the SECRET level: YES NO.

3) Is the Access control system encoded, and are ID data and PINs restricted to SAP-indoctrinated personnel: YES NO.

4) Do external access control devices outside SAPF have tamper protection? YES NO.

5) Is the access control device integrated with an IDS? YES NO N/A
Is the access control device integrated with a network system? YES NO N/A

2. Does the SAPF have windows? YES NO

a. Are they acoustically protected? YES NO N/A

If YES, how? Please explain: _____

b. Are they secured against forced opening? YES NO N/A

If YES, how? Please explain: _____

c. Are they protected against visual surveillance? YES NO N/A

If YES, how? Please explain: _____

Classification



3. Do ventilation ducts penetrate the SAPF perimeter? YES NO *(Indicate all duct penetrations and their size on a separate floor plan as an attachment.)*

a. Are any ducts over 96 square inches at the point of egress? YES NO

If YES, how are they protected: IDS (Describe in Section E), Bars/Grills/Metal Baffles, OTHER, please explain: _____

b. Inspection Ports: YES NO

If YES, are they within the SAPF? YES NO

If NO, are they secured? YES NO; Please Explain: _____

c. Do all ventilation ducts penetrating the perimeter meet acoustical requirements? YES NO

(Note: All ducts and vents, regardless of size may require acoustical protection.) If yes, how are they protected: Metal Baffles: , Noise Generator: , Z-Duct: , Other (Describe) _____

4. Construction:

a. Perimeter wall Material and Thickness: _____

Do the walls extend from the true floor to the true ceiling? YES NO.

b. True ceiling (material and thickness): _____

c. False ceiling? YES NO

If YES, what is the type of ceiling material? _____

What is the distance between false and true ceiling? _____

d. True floor (material and thickness): _____

e. False Floor? YES NO

If YES, what is the type of false flooring? _____

What is the distance between the false and true floor? _____

5. Remarks:

Classification



Section D – Doors

1. Describe SAPF Primary Entrance Door Construction (Indicate on floor plan):

a. Does the door and door frame meet sound attenuation requirements? YES NO
If NO, have acoustical countermeasures been employed? YES NO
Please explain: _____

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

c. Is a door sweep/thresholds installed? YES NO
If NO, explain: _____

d. Is an acoustical/astragal strip installed? YES NO
If NO, explain: _____

2. Describe number and type of doors used for SAPF emergency exits and other perimeter doors including day access (Show on floor plan):

a. Do the doors and doorframes meet sound attenuation requirements? YES NO
If NO, have acoustical countermeasures been employed? YES NO
Please explain: _____

b. Has exterior hardware been removed? YES NO
If NO explain: _____

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

4. Locking devices:

a. Primary SAPF Entrance Door: List combination lock manufacturer, model number, and Group rating: _____. Does the entrance door stand open into an uncontrolled area? YES NO
If YES, describe tamper protection: _____

b. Emergency Exits and Other Perimeter Doors: Describe (locks, metal strip/bar, deadbolts, and panic hardware): _____

c. Where are the door lock combinations filed? (Please identify the SAPF PSO and SAPF ID #)

5. Remarks: _____

Classification



Section E – Intrusion Detection Systems (IDS)

1. General IDS Description:

a. IDS Company provider Name (If applicable) _____

b. Premise Control Unit (PCU): Manufacturer: _____
Model Number: _____ Tamper Protection: YES NO

c. Is the PCU located inside the SAPF perimeter (Indicated on floor plan)? YES NO
If NO, please explain: _____

d. Balanced Magnetic Switch (BMS):

1) Manufacturer: _____

2) Model Number: _____

3) Tamper Protection: YES NO

e. Location of interior motion detection protection: Accessible points of entry / perimeter? YES NO
SAP Storage Areas? YES NO

f. Motion Sensors (Indicate sensor placement on a legible floor plan; 8.5" x 11" or 11" x 17" paper):

1) Manufacturer: _____

2) Model Number: _____

3) Tamper Protection: YES NO

4) Are motion sensors installed above the false ceiling? YES NO N/A

5) Are motion sensors installed below the false floor? YES NO N/A

g. Are there any other intrusion detection equipment sensors / detectors in use? YES NO
Please identify make, model, and manufacturer and function (Indicate on floor plan):

h. Does the IDS extend beyond the SAPF perimeter? YES NO
Can the status of the PCU be changed from outside IDS protection? YES NO
If YES, is an audit conducted daily? YES NO
Has the IDS configuration been approved by the PSO? YES NO

i. Do any intrusion detection equipment components have audio or video capabilities? YES NO
If YES, please explain: _____
Has the PSO granted a waiver for this capability? YES NO

Classification



j. IDS Administrator SAP indoctrinated? YES NO

k. External Transmission Line Security: What is the method of line security?

128-bit (or greater) Encryption YES NO

If YES, has the encryption been certified by National Institute of Standards and Technology (NIST) or another independent testing laboratory? YES NO

If not 128-bit (or greater) encryption, is there an alternate? YES NO

If YES, please explain: _____

Does the alternate line utilize any cellular or other Radio Frequency (RF) capability?

YES NO

Manufacturer: _____

Model Number: _____

l. Does any part of the IDS use a Local or Wide Area Network (LAN/WAN)? YES NO N/A

1) Is the *Network Intrusion Detection Software* (NIDS) administrator at least TOP SECRET (collateral) cleared? YES NO N/A

2) Is the host computer dedicated solely for security purposes? YES NO N/A

3) Is the host computer secured within an alarmed area controlled at the SECRET or higher level? YES NO N/A

4) Is the host computer protected through firewalls or similar devices? YES NO N/A
Are the firewalls / devices configured to only allow data transfers between IDS components? YES NO N/A

5) Is the password for the host computer unique for each user and at least 8-characters long? YES NO N/A

6) Is the password changed semi-annually? YES NO N/A

7) Are remote security terminals protected the same as host computer? YES NO N/A.
If NO, please explain: _____

m. Was the IDS installed by US citizens? YES NO N/A

If NO, explain: _____

2. Is Emergency Power available for the IDS? YES NO N/A

What type? Generator: YES NO

If YES, how many hours? _____

Battery: YES NO

If YES, how many hours? _____

Classification



3. Describe the method of ventilation and duct work protection (If applicable from Annex A, Section 3C):

4. Where is the IDS Alarm Monitor Station located? _____

5. Has the IDS Alarm Monitor Station been installed to Underwriters Laboratories certified standards?

YES NO

If YES, provide certification Number # _____ and expiration date _____ of UL certification.

6. Does the Monitor Station have any remote capabilities (i.e., resetting alarms, issuing PINs, accessing/securing alarms, etc)? YES NO N/A

If YES, explain: _____

7. Does the IDS have any automatic features (i.e., timed auto-secure, auto-access capabilities)?

YES NO N/A

8. Does the PCU/Keypad have dial out capabilities? YES NO

9. IDS Response Personnel:

a. Who provides initial alarm response? _____

b. Does the response force have a security clearance? YES NO

If YES, what is the clearance level? _____

c. Emergency Procedures documented? YES NO

d. Reserve Security Force available? YES NO

e. Response to an alarm condition: _____ minutes.

f. Are response procedures tested and records maintained? YES NO

If NO, please explain: _____

g. If required, has a Catastrophic Failure Plan been approved by the PSO? YES NO

Classification



10. Has the IDS passed PSO or UL 2050 installation and acceptance tests? YES NO

If YES, attach a copy of certificate.

11. Does the IDS undergo semiannual testing? YES NO

12. Have IDS records been maintained? YES NO

If NO, please explain: _____

13. Remarks: _____

Classification



Section F – Telecommunication Systems and Equipment Baseline

1. Is the facility declared a “No Classified Discussion Area”? YES NO

(If YES, then the audio protection questions within of this section may be identified as N/A.)

If the facility is declared a No Classified Discussion Area, are warning notices posted prominently within the facility? YES NO N/A

2. Does the facility have any unclassified telephones that are connected to the commercial Public Switch Telephone Network (PSTN)? YES NO

a. What is the method of on-hook audio protection?

1) TSG-6 approved telephone or instrument? YES NO N/A

(Please identify all telephone equipment/stations and/or instruments being used either below or as an attachment.)

- Manufacturer: _____
- Model number: _____
- TSG number (If applicable): _____

2) TSG-6 approved disconnect device? YES NO N/A

a) Line Disconnect: YES NO N/A

b) Ringer Protection: YES NO N/A

- Manufacturer: _____
- Model number: _____
- TSG number: _____

3) TSG-2 Configured Computerized Telephone System (CTS)? YES NO N/A

a) If YES, please provide the following information about the CTS:

Manufacturer: _____

Model: _____

b) If YES, please provide specific location of the CTS: _____

c) Is access to the facility housing the CTS physically controlled? YES NO

Classification



d) If YES, what is the clearance level (if any) of facility or area where the switch is located and how is area controlled? _____

e) Are all cables, signal lines and intermediate wiring frames between the SAPF telephones and the CTS physically protected or contained within a physically controlled space? YES NO

If NO, please explain: _____

f) Are all program media, such as tapes and/or disks, from the CTS afforded physical protection from unauthorized alterations? YES NO

g) Is an up-to-date master copy of the CTS software program maintained for confirmation and/or reloading of the operating system? YES NO

h) Does the CTS have the capability to force or hold a telephone station off-hook? YES NO

i) Does the CTS use remote maintenance and diagnostic procedures or other remote access features? YES NO

If YES, explain maintenance procedures: _____

j) Do the CTS installers and programmers have security clearances? YES NO

If YES, at what access level (minimum established by PSO): _____

If NO, are escorts provided? YES NO

4) Is it an Internet Protocol phone system (IPS) (Ref TSG-2(B))? YES NO N/A

a) If YES, please provide the following information about the IPS:

• Manufacturer: _____

• Model: _____

• IPS Location: _____

b) Is access to the facility housing the IPS physically controlled? YES NO

c) If YES, what is the clearance level (if any) of facility or area where the switch is located at and how is area controlled? _____

d) Are all cables, signal lines and intermediate wiring frames between the SAPF telephones and the IPS physically protected or contained within a physically controlled space? YES NO

If NO, please explain: _____

Classification



e) Are all program media, such as tapes and/or disks, from the IPS afforded physical protection from unauthorized alterations? YES NO

f) Is an up-to-date master copy of the IPS software program maintained for confirmation and/or reloading of the operating system? YES NO

g) Does the IPS have the capability to force or hold a telephone station off-hook? YES NO

h) Does the IPS use remote maintenance and diagnostic procedures or other remote access features? YES NO

If YES, explain maintenance procedures: _____

i) Do the IPS installers and programmers have security clearances? YES NO

If YES, at what access level (minimum established by PSO): _____.

If NO, are escorts provided? YES NO

b. Do all unclassified telephones within the facility have a hold, mute and/or push-to-talk [handset] capability, (for **off-hook audio protection**)? YES NO N/A

If NO, please explain: _____

3. Automatic telephone call answering:

a. Are there any automatic call answering devices for the telephones in the SAPF? YES NO

1) If YES, please identify the type:

a. Voice mail/ unified message service YES NO

b. Standalone Telephone answering device (TAD) YES NO

2) Provide manufacturer and model number of the equipment. _____

b. Are speakerphones/microphones enabled? YES NO N/A

If YES, has the remote room monitoring capability been disabled? YES NO

Has this been approved for use by the PSO? YES NO N/A

Provide detailed configuration procedures: _____

c. If applicable, is the voice mail or unified messaging services configured to prevent unauthorized access from remote diagnostic ports or internal dial tone? YES NO

4. Are any Multi-Function Office Machines (M-FOMs) used within the SAPF (M-FOMs are electronic equipment that can be used as network or standalone printers, facsimile, and copiers)?

YES NO

a. If YES, please identify the device to include: *(Please identify all M-FOM devices in use, either below or as an attachment. (include a manufacture Volatile statement for each M-FOM)*

Make _____ Model _____ S/N: _____

Classification



b. If YES, please identify all features and information processing levels of the M-FOM:

1) Copier: YES NO N/A. If YES, level(s) of information: _____

2) Facsimile: YES NO N/A. If YES, level(s) of information: _____

3) Printer (connected to a stand-alone computer or network): YES NO N/A
(If YES, please explain and identify the system(s) and the level(s) of information)

c. Does the M-FOM have memory storage capability? YES NO

If YES, what kind? Volatile (information in memory clears when powered off)

Non-volatile (information in memory remains when powered off)

d. Does the M-FOM have a digital hard drive? YES NO N/A

e. Have maintenance and disposition procedures been established? YES NO N/A

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

g. Does the M-FOM have voice transmission capability and/or a telephone handset?

YES NO N/A.

If YES, how is this feature protected? Please describe. _____

5. Are there any Video Teleconference (VTC) Systems installed? YES NO. If YES, what level(s) of information is the VTC system processing? _____; Which room(s) contain VTC systems? _____

6. Are there any commercial television receivers installed? YES NO

IF YES, provide a separate annotated floor plan of the commercial Television system.

7. Are all telecommunications systems, devices, features, and software documented? YES NO

(Attached telecommunication baseline)

8. Does the SAPF have any automated environmental infrastructure systems? YES NO

IF YES, Describe what Countermeasure have been taken to provide protection against malicious activity, intrusion, and exploitation. (Example: premise management systems, environmental control systems, lighting and power control units, uninterrupted power sources)

9. Remarks: _____

Classification



Section G – Acoustical Protection

1. Do all areas of the SAPF meet acoustical protection requirements of Annex E? YES NO

If NO, describe additional measures taken to provide conforming acoustical protection (e.g., added sound insulation, door and windows coverings, stand-off areas, sound masking, etc):

2. Are there any amplified audio systems used for classified information? (Example: VTC, P.A Systems, etc.) YES NO

If YES, are the walls/ceilings/floor of the room where the amplified audio system resides acoustically treated to meet a *Sound Transmission Class* (STC) of 50 or better? YES NO N/A

3. Is there a public address or music system entirely contained within SAPF? YES NO

If YES, provide a separate annotated floor plan for each system.

4. Is the SAPF equipped with a public address, emergency / fire announcement or music system originating outside the SAPF? YES NO

If YES, provide a separate annotated floor plan for each system including indicated location of system isolation equipment (include manufacturer, model, specifications and UL conformance data)

Note: PSO's Certified TEMPEST Technical Authority review maybe required.

Classification



Section H – Classified Destruction Methods

1. Destruction Methods

a. Describe the method and equipment used for destruction of classified/sensitive material (if more than one method or device, use Remarks to describe: (If more than one device, use Remarks to list all manufacturer and model)

Method _____ Device Manufacturer _____ Model _____

b. Is a secondary method of destruction available? YES NO

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

d. Describe method or procedure used for handling non-soluble classified/sensitive material at this facility: _____

e. Have provisions been made for the emergency destruction of classified / sensitive program material? (If required) YES NO N/A

2. Remarks: _____

Classification



Section I – TEMPEST/Technical Security

1. Does the facility electronically process classified information? YES NO
If YES, what is the highest level of information processed? _____

2. For the last TEMPEST Accreditation (if applicable), provide the following information:
Accreditation granted by: _____ on _____

3. Has the PSO's *Certified TEMPEST Technical Authority (CTTA)* required any TEMPEST countermeasures? YES NO N/A
If YES, please identify the countermeasures that have been installed (i.e., non-conductive sections, Radio Frequency (RF) shielding, power/signal line filters, window film, etc.): _____

4. Are there any other systems installed within or in close proximity to the SAPF that have RF transmit capability (e.g. fire alarm, ground-to-air radio, Cellular tower, RF networks etc.)? YES NO
If YES, please explain: _____

Classification



JOINT AIR FORCE - ARMY - NAVY (JAFAN) MANUAL 6/9

Annex B - Intrusion Detection Systems (IDS)

This Annex sets forth the requirements and establishes the Standard for Intrusion Detection Systems (IDS) and associated operations for Government and Government-Sponsored Special Access Program Facilities (SAPFs). Compliance with these requirements is mandatory for all SAPFs established after the effective date of this Manual.

1.0 IDS Overview. The IDS shall detect attempted or actual unauthorized human entry into a SAPF. The IDS complements other physical security measures. The IDS shall consist of three distinct components: Intrusion Detection Equipment (IDE), Security and Response-Force Personnel, and Security Operation Procedures. IDS operations shall comprise four phases as described below:

1.1 Detection Phase. The detection phase begins when a sensor reacts to the stimuli for which the sensor was designed to detect.

1.2 Reporting Phase. The Premise Control Unit (PCU) receives signals from all associated sensors in the SAPF's alarmed zone and establishes the alarm status. The alarm status is immediately transmitted to the Monitoring Station. Within the Monitoring Station, a dedicated Alarm-Monitoring panel (or central processor) monitors incoming PCU signals. On receiving an alarm signal, a Monitoring Station's enunciator generates an audible and visible alarm for the monitoring personnel.

1.3 Assessment Phase. The assessment phase is the initial phase requiring human interaction. On receiving an audible or visible alarm, monitoring personnel immediately assess the situation and determine the appropriate response.

1.4 Response Phase. The response phase begins immediately after the operator has assessed the alarm condition. All alarms shall be immediately investigated. During the response phase, the precise nature of the alarm shall be determined and appropriate measures taken to safeguard the SAPF.

2.0 Definitions

2.1 Alarm. A visual and audible indication that a sensor has detected the unauthorized breach into a SAPF. Alarms also signify the malfunction of a sensor that normally causes such an alarm.

2.2 Alarm Zone. An alarm zone is a segregated or specified area under the control of a single Premise Control Unit (PCU).

2.3 Intrusion Detection Equipment (IDE). IDE is all the equipment, associated software/firmware, and communication lines included within the IDS.

2.4 Monitoring Station. The monitoring station is the central point for collecting alarm status from the PCUs handling the alarm zones under control of an IDS.

2.5 Premise Control Unit (PCU). A PCU is a device that receives changes of alarm status from IDS sensors, and transmits an alarm condition to the monitoring station.

2.6 Security in-depth. A determination by the Program Security Officer (PSO) that a facility's security programs consist of layered and complementary controls sufficient to deter and detect unauthorized entry and movement within a SAPF.

2.7 Sensor. Sensors are devices that respond to a physical stimulus (as heat, light, sound, pressure, magnetism, or a particular motion) and transmits a resulting impulse.

2.8 United States. As used herein, the United States includes the 48 contiguous states, Alaska, Hawaii, as well as, protectorates, territories, and possessions under control of the United States (e.g., Puerto Rico, Guam, Wake, Midway, American Samoa, US Virgin Islands, others). This definition does not include US-controlled installations (for example, military bases, embassies, leased space) located in foreign countries.

3.0 IDS Requirements. This section specifies the requirements for Intrusion Detection Systems (IDS) and associated operations for government and



government-sponsored SAPFs and other associated areas.

3.1 General IDS Requirements. The following general requirements apply to all SAPFs and shall be met as a prerequisite for using a SAPF for government-classified operations.

3.1.1 SAPF Protection. ~~All areas of a SAPF where SAP material is stored shall be protected by an IDS, unless continuously occupied.~~ All areas of a SAPF that reasonably afford access to the SAPF, or where SAP is stored, shall be protected by an IDS, unless continuously occupied. (Ch#1) If the occupants of a continuously occupied SAPF cannot observe all potential entrances to the SAPF, the SAPF shall be equipped with a system to alert occupants of intrusions into the SAPF. This alerting system shall consist of appropriate sensors. IDE and cabling associated with the alerting system shall not extend beyond the perimeter of the SAPF. Emergency exit doors shall be monitored 24 hours a day to provide quick identification and response to the appropriate door when there is an alarm indication (see paragraph 6.1.3).

3.1.2 Independent IDE and IDS. SAPFs shall be provided with IDE and alarm zones that are independent from systems safeguarding other protected sites. If a single monitoring station supervises several alarm zones, then the audible and visible annunciation for each such zone shall be distinguishable from other zones. The IDS's PCU, associated sensors, and cabling protecting the SAPF, shall be separate from and independent of fire, smoke, radon, water, and other such systems. (Note: If an access control system is integrated into an IDS, reports from the access control system shall be subordinate in priority to reports from intrusion alarms.)

3.1.3 Security During Catastrophic Failure of IDS. If any of the components of an IDS encounters a catastrophic failure to the extent that the IDS can no longer provide essential security services, then SAPF indoctrinated personnel shall provide security by physically occupying the SAPF until the IDS returns to normal operation. As an alternative, the outside SAPF perimeter shall be continuously protected by the response force or a guard force until the IDS returns to normal operation. If neither of these alternatives is possible, a catastrophic failure plan shall be submitted in writing to the PSO for review and approval prior to implementation. (See paragraph 6.1.2.) Examples of catastrophic failure are: loss of line security/communication, loss of

alarm services, inoperability of IDS, loss of both primary and emergency power, or other such failure.

3.1.4 Safeguarding IDE, Key Variable(s), and Passwords. System administration key variables and operational passwords shall be protected and restricted to SAP-indoctrinated personnel granted a final security clearance commensurate with the Program being protected. In areas outside of the United States, procured IDE shall remain solely under US control, or as otherwise authorized by the PSO in writing.

3.1.5 IDE Acceptability. All IDE must comply with UL-2050 or equivalent as approved by the PSO in writing. Prior acceptance by the PSO does not constitute approval for use within another SAPF. Contractors shall comply with UL 2050 by maintaining an active UL certificate of installation and service. With sufficient justification, the PSO may issue written waivers to UL 2050. Any IDE that could allow unintentional audio or other intelligence-bearing signals in any form to pass beyond the confines of the SAPF is unacceptable and prohibited for IDS installation. IDE shall not include audio or video monitoring without appropriate countermeasures and PSO approval. ~~IDS comprised of IDE with auto-reset features shall have the auto-reset capability disabled as required in paragraph 3.2.7.~~ ISA comprised of IDE with auto-reset features may be used with the concurrence of the PSO. (Ch#1)

3.1.6 IDS Approval. The PSO shall approve IDS proposals and plans prior to installation within a SAPF as part of the initial SAPF construction approval process. Final IDS acceptance tests as described herein and as prescribed in applicable manufacturer's literature shall be included as part of the SAPF accreditation package. Accreditation files for the SAPF shall be maintained as described in paragraph 6.3. The PSO shall approve the IDS prior to use for government or government-sponsored SAPFs.

3.2 Detailed IDS Requirements. The following detailed requirements apply to all SAPF IDSs.

3.2.1 Sensors. All sensors protecting a SAPF shall be located within that SAPF. Any failed IDE sensor shall cause an immediate and continuous alarm condition until the failure is corrected or compensated.

3.2.1.1 Motion Detection Sensors. All areas of a SAPF that reasonably afford access to the SAPF,



or where SAP material is stored, and that are not accredited for continuous operation shall be protected with UL-listed, equivalent or PSO approved motion detectors (see paragraph 3.1.1). Sufficient detectors shall be installed to assure meeting the requirements of paragraph 4.2.1. Within the US motion detection sensors are normally not required above false ceilings or below false floors; however, these detectors may be required by the PSO for such areas outside of the US.

3.2.1.2 Entrance Door Delay. Entrance door sensors may have an initial time delay built into the IDS to allow for change in alarm status, but shall not exceed 30 seconds.

3.2.1.3 SAPF Perimeter Sensors. With PSO approval, sensors supporting the external SAPF perimeter and perimeter equipment (if used) may be connected to the SAPF IDS provided the lines are installed on a separate zone and routed within grounded EMT or metallic conduit.

3.2.1.4 Perimeter Door Sensor. Each SAPF perimeter door shall be protected by a Balanced Magnetic Switch (BMS) installed in accordance with section 4.1.2.

3.2.1.5 Emergency Exit-Door Detectors. The BMS installed on emergency exit doors shall be monitored 24 hours a day.

3.2.1.6 Dual-Technology Sensors. The use of dual-technology sensors is authorized when each technology transmits alarm conditions independent from the other technology.

3.2.2 Premise Control Units and Access Control Switches. PCUs shall be located within the SAPF to ensure that only SAPF personnel can initiate a change between *access* and *secure* mode. The means of changing between access and secure modes shall be located within the SAPF. Operation of the access/secure switch shall be restricted by using a device or procedure that verifies authorized PCU use. Any polling from the monitoring station to the PCU shall not exceed six minutes regardless of access state.

3.2.3 Communications between Sensors and the PCU. Cabling between the sensors and the PCUs shall be dedicated to the IDE and contained within the SAPF. Alternately, if the wiring cannot be contained within the SAPF, such cabling shall meet the transmission requirements of paragraph 3.2.8. All IDE cabling internal to the SAPF shall comply with national and local

code standards. If applicable, the cabling shall be installed in accordance with TEMPEST and COMSEC requirements. Outside of the United States, if determined by the PSO, wiring will be protected within EMT or metallic conduit. The use of wireless communications between sensors and PCU is normally prohibited. However, under exceptional circumstances, when such cabling is not possible or feasible, the wireless communications maintain continuous connection and are impervious to jamming, manipulation, and spoofing and meets other security requirements of this Annex, the PSO may authorize in writing the use of wireless communications between sensors and the PCU. Co-utilizing agencies shall be notified of any such exception.

3.2.4 Monitor Station and Panel. Alarm status shall be provided at the monitoring station. The alarm-monitoring panel shall be designed and installed in a location that prevents observation by unauthorized persons. If an Access Control System (ACS) is integrated with an IDS, reports from the ACS shall be subordinate in priority to reports from intrusion alarms (see paragraph 3.1.2).

3.2.5 Alarms. Alarm annunciations shall exist for the below listed alarm conditions. A false/nuisance alarm is any alarm signal transmitted in the absence of a detected intrusion such as alarms caused by changes in the environment, equipment malfunction, operator failure, animals, electrical disturbances, or other such causes. False/nuisance alarms shall not exceed one alarm per 30-day period per zone. (See paragraph 5.3.3.)

3.2.5.1 Intrusion Alarm. An intrusion or attempted intrusion shall cause an immediate and continuous alarm condition.

3.2.5.2 Failed-Sensor Alarm. A failed IDE sensor shall cause an immediate and continuous alarm condition.

3.2.5.3 Maintenance Alarm. The IDS, when in the maintenance mode, shall cause an immediate and continuous alarm (or maintenance message) throughout the period the IDS is in the maintenance mode. Zones that are shunted or masked shall also cause such an alarm. (See paragraph 3.2.10.3 for additional requirements.)

3.2.5.4 Tamper Alarm. The IDS, when sustaining tampering, shall cause an immediate and continuous alarm. (See paragraph 3.2.12 for additional requirements.)



3.2.5.5 Failed/Changed Electrical Power Alarm. Equipment at the monitoring station shall visibly and audibly indicate a failure in a power source, a change in power source, and the location of the failure or change. (See paragraph 3.2.11.2 for additional requirements.)

3.2.6 IDS Event (Alarm) Log. The IDS shall have a means for providing a historical record (items specified in paragraph 6.2.2) of all events through an automatic logging system. If the IDS has no provision of automatic entry into archive, as an alternative, a manual logging system shall be maintained in accordance with paragraph 6.2.2.

3.2.7 Alarm Reset. ~~All alarm activations shall be reset using designated personnel. An IDS with an auto-reset feature shall have the auto-reset feature disabled.~~ All alarm activations shall be reset using designated personnel unless the auto reset feature has been approved by the PSO. (Ch#1)

3.2.8 External Transmission Line Security. When any IDS transmission line leaves a SAPF, line security shall be employed. The UL 2050 certificate shall state that line security has been employed. The following types of line security are acceptable:

3.2.8.1 Encrypted Lines. Encrypted-line security is achieved by using an approved 128-bit (or greater) encryption algorithm. The algorithm shall be certified by NIST or another independent testing laboratory.

3.2.8.2 Alternative Lines. If the communication technology described in 3.2.8.1 is not available, the SAPF owner and the PSO shall coordinate an optional supervised communication scheme. The communication scheme shall be adequately supervised to protect against modification and substitution of the transmitted signal.

3.2.9 Networked IDSs. In those cases in which an IDS has been integrated into a LAN or WAN, the following requirements shall be met. (See paragraphs 5.3.5 and 5.5.3.)

3.2.9.1 Dedicated IDS (Host) Computer. The IDS application software shall be installed and run on a host computer dedicated to security systems. The host computer shall be located in an alarmed area controlled at the SECRET or higher level.

3.2.9.2 IDS Host Computer Communications. All host computer communications to the LAN/WAN

shall be protected though firewalls, or similar enhancements, that are configured to only allow data transfers between IDS components.

3.2.9.3 User IDs and Passwords. A unique user ID and password is required for each individual granted access to the IDS host computer. Passwords shall be a minimum of eight characters; consist of alpha, numeric, and special characters; and shall be changed a minimum of every six months.

3.2.9.4 Computer Auditing and Network Intrusion Detection. Computer auditing and network intrusion detection software (NIDS) shall monitor and log access attempts and all changes to IDS applications. Additionally, NIDS and IDS administrators shall be immediately notified of unauthorized modifications. The NIDS administrator shall possess a minimum of a TOP SECRET clearance and IDS system administrator shall be SAP-indoctrinated.

3.2.9.5 LAN/WAN Transmissions. All transmissions of IDS information over the LAN/WAN shall be encrypted using a NIST-approved algorithm with a minimum of 128-bit encryption.

3.2.9.6 Remote Terminals. Remote networked IDS terminals shall meet the following requirements: (a) Remote terminals shall be protected within a SAPF. (b) SAP-indoctrinated personnel shall ensure that personnel with access to the remote terminal are not able to modify Intrusion Detection System/Access Control System (IDS/ACS) information for areas for which they do not have access. (c) Each remote terminal shall require an independent user ID and password in addition to the host login requirements. (d) Network intrusion detection and auditing software shall log and monitor failed logins and IDS/ACS application program modifications.

3.2.10 IDS Modes of Operation. The IDS shall have three modes of operation: access mode, secure mode, and maintenance mode as described below. A fourth mode "Remote Service Mode" shall not exist unless the requirements of 3.2.10.4 are met. There shall be no capability for changing the mode of operation or access status of the IDS from a location outside the SAPF unless SAPF personnel conduct a daily audit of all openings and closings. Changing Access/Secure status of a SAPF shall be limited to SAP indoctrinated personnel. IDS modes shall meet the following requirements:



3.2.10.1 Access Mode. During access mode, normal authorized entry into the facility in accordance with prescribed security procedures shall not cause an alarm. Tamper and emergency exit door circuits shall remain in the secure mode of operation.

3.2.10.2 Secure Mode. In the secure mode, any unauthorized entry into the SAPF shall cause an alarm to be immediately transmitted to the monitoring station.

3.2.10.3 Maintenance Mode and Zone Shunting/Masking. When an alarm zone is placed in the maintenance mode, a signal for this condition shall be automatically sent to the monitoring station. This signal shall appear as an alarm (or maintenance message) at the monitoring station and shall continue to be displayed visibly at the monitoring station throughout the period of maintenance. The IDS shall not be securable while in the maintenance mode. All maintenance periods shall be archived in the system. The PSO may require that a maintenance Personal Identification Number (PIN) be established and controlled by SAP personnel. Additionally, a shunted or masked zone or sensor shall be displayed as such at the monitoring station throughout the period the condition exists. (See paragraph 6.2.3 for logging requirements.)

3.2.10.4 Remote Service Mode. After the initial installation, the capability for remote diagnostics, maintenance, or programming of IDE shall not exist unless accomplished by personnel granted a final SECRET clearance appropriately SAP-indoctrinated and shall be properly logged or recorded in the Remote Service Mode Archive. A self-test feature shall be limited to one second per occurrence. (See paragraph 5.5.3.)

3.2.11 Electrical Power. Primary electrical power for all IDE shall be commercially supplied in alternating current (AC) or direct current (DC) form. In the event such commercial power fails, the IDE shall automatically transfer to an emergency electrical power source without causing an alarm indication.

3.2.11.1 Emergency Backup Electrical Power. Emergency backup electrical power for the SAPF and monitoring station shall be provided by battery, generator, or both. If batteries are provided for emergency backup power, they shall provide a minimum of 24 hours (UL 1076) of backup power and they shall be maintained at full charge by automatic charging circuits. (See paragraph 5.3.4.)

3.2.11.2 Electrical Power Source and Failure Indication. An audible and visual indicator at the PCU shall provide an indication of the electrical power source in use (AC or DC). Equipment at the monitoring station shall visibly and audibly indicate a failure in a power source, a change in power source, and the location of the failure or change.

3.2.12 Tamper Protection. All IDE within the SAPF shall be equipped with tamper detection devices. The tamper detection shall be monitored continuously whether the IDS is in the access or secure mode of operation.

4.0 Installation and Acceptance Testing Requirements. This section specifies the requirements for IDS installation and testing. Additionally, IDE installation and testing shall meet the following requirements:

4.1 Installation Requirements. The IDE shall be installed in a manner that assures conformance with all requirements of sections 3.1 and 3.2 of this standard and the following specific requirements. US citizens shall accomplish all IDE installation.

4.1.1 Motion Detector Installation. Motion detection equipment shall be installed in accordance with manufacturer specifications meeting UL standards.

4.2 Acceptance Testing. The IDE shall be tested to provide assurances that it meets all requirements of sections 3.1 and 3.2 of this standard and those detailed tests specified below. All SAPF IDS sensors shall be tested and found to meet the requirements herein prior to SAPF accreditation. Records of testing and test performance shall be maintained in accordance with paragraph 6.2.1. US citizens shall accomplish all IDE testing.

4.2.1 Motion Detection Sensor Testing. Test all motion detection sensors to ensure that the sensitivity is adjusted to detect an intruder who walking toward/across the sensor at a minimum of four consecutive steps at a rate of one step per second. That is, 30 inches \pm 3 inches or 760 mm \pm 80 mm per second. The four-step movement shall constitute a "trial." An alarm shall be initiated in at least three out of every four such consecutive "trials" made moving progressively through the SAPF. The test is to be conducted by taking a four-step trial, stopping for three to five seconds, taking a four-step trial, stopping for three to five seconds, repeating the process throughout the SAPF.



Whenever possible, the direction of the next trial is to be in a different direction.

4.2.2 BMS Testing. All BMSs shall be tested to ensure that an alarm signal initiates before the non-hinged side of the door opens beyond the thickness of the door from the seated position. That is, the sensor initiates after the door opens 1 3/4 inch for a 1 3/4 inch door.

4.2.3 Tamper Testing. Remove each IDE cover individually and ensure that there is an alarm indication on the monitoring panel in both the secure and access modes. Tamper detection devices need only be tested upon installation with the exception of the tamper detection on the PCU that is activated when it is opened. The PSO may require more frequent testing of tamper circuits. (See paragraph 5.4 for tamper testing of PCU.)

4.2.4 Manufacturer's Prescribed Testing. All tests prescribed in manufacture's literature shall be conducted to ensure that the IDE operates in accordance with manufacture's specifications and applicable requirements specified herein.

5.0 Operation, Maintenance, and Semi-Annual Testing Requirements. The IDS shall be operated and maintained to assure that the requirements of sections 3.1 and 3.2 of this standard are met. Additionally, IDE operation and maintenance shall meet the following requirements:

5.1 Monitoring

5.1.1 Monitoring Station Staffing. The monitoring station shall be continuously supervised and operated by US citizens who are trained alarm monitors, cleared to the SECRET level.

5.1.2 Monitoring Station Operator Training. Monitoring station operators shall be trained in IDE theory and operation to the extent required to effectively interpret incidents generated by the IDE and to take proper action when an alarm activates.

5.2 Response

5.2.1 Alarm-Condition Response. All alarms shall be investigated and the results documented. Every alarm condition shall be considered a detected intrusion until resolved. The response force shall take appropriate steps to safeguard the SAPF as permitted by a written support agreement (see paragraph 6.1.3), local law enforcement, and

circumstances surrounding the event until properly relieved (see paragraph 5.5.4). (Note: The primary purpose of any alarm response team is to ascertain if intrusion has occurred and if possible assist in the apprehension of the individuals. If an alarm activation resets in a reasonable amount of time, no physical penetration of the area or container is visible, then entrance into the area or container is not required. Therefore the initial response team may consist of uncleared personnel. If the alarm activation resets within 15 minutes for closed storage and 5 minutes for open storage and no physical penetration is observed, a SAP-indoctrinated individual will record the incident and complete a physical review of the SAPF at the beginning of the next working day. If the alarm activation does not reset, or physical penetration is observed, then a cleared response team must be dispatched. The initial uncleared response team must stay on station until relieved by a cleared response team. If a cleared response team does not arrive within one hour, then a report to the PSO must be made by the close of the next business day.) A SAP-indoctrinated individual must arrive as soon as possible, but not to exceed 60 minutes, to conduct an internal inspection of the SAPF, attempt to determine the probable cause of the alarm activation and reset the IDS prior to the departure of the response force. The response team must stay on station until arrival of a SAP-indoctrinated individual and an internal inspection of the SAPF has been conducted. For SAPFs located within the US, the response force shall arrive at the SAPF within:

- Open Storage: 5 minutes
- Closed Storage: 15 minutes

For SAPFs located outside of the United States, security in-depth must be used and cleared or US Government personnel shall arrive at the SAPF within:

- Open Storage: 5 minutes
- Closed Storage: 10 minutes

5.2.2 Response-Force Personnel Training and Testing. Response Force Personnel shall be appropriately trained and equipped according to SOPs to accomplish initial or follow-up response to situations that may threaten the SAPF's security. Such personnel may include local law enforcement support or other external forces as stated in formal agreements. Coordinated response force testing shall be conducted semi-annually. False alarm activations may be used in lieu of a response-force



test provided the proper response times were met. A record of response-force personnel testing shall be maintained for a minimum of two years.

5.3 Maintenance

5.3.1 Maintenance Staffing. ~~The IDE shall be maintained by US citizens who have been subjected to a trustworthiness determination (favorable NAC with no clearance required). Non-US citizens shall not provide these services without prior written approval by the PSO.~~ The IDE shall be maintained by US citizens. Non-US citizens shall not provide these services without prior written approval by the PSO. (Ch#1)

5.3.2 Sensor Adjustment or Replacement. Sensors that do not meet prescribed requirements shall be adjusted or replaced as needed to assure that the requirements of sections 3 and 4 of this standard are continually met.

5.3.3 False Alarm Prevention. The maintenance program for the IDS shall ensure that false-alarm incidents do not exceed one in a period of 30 days per alarm zone.

5.3.4 Emergency-Power Battery Maintenance. The battery manufacturer's periodic maintenance schedule shall be followed and the results documented.

5.3.5 Network Maintenance. If the IDS is connected to a network, the IDS and NIDS system administrator shall maintain configuration control, ensure the latest operating system security patches have been applied, and shall configure the operating system to provide a high level of security. (See paragraph 3.2.9.)

5.4 Semiannual IDE Testing. The IDE shall be tested semiannually (every six months) to provide assurances that the IDS is in conformance with the requirements of paragraphs 4.2.1 through 4.2.4. Records of semiannual testing and test performance shall be maintained in accordance with paragraph 6.2.1. US citizens shall accomplish all IDE testing. Non-US citizens shall not provide such testing services without prior written approval by the PSO.

5.5 Operational Requirements Limited to SAP Indoctrinated Personnel

5.5.1 Changing Access/Secure Status. Changing Access/Secure status of the SAPF shall be limited to SAP-indoctrinated personnel.

5.5.2 IDS Administrator. If the IDS is connected to a network, the IDS system administrator shall maintain configuration control, ensure the latest operating system security patches have been applied, and shall configure the operating system to provide a high level of security.

5.5.3 Remote Operations. After initial installation, remote diagnostics, maintenance, or programming of the IDE shall not be accomplished unless accomplished by personnel granted a final SECRET clearance appropriately SAP-indoctrinated and shall be appropriately recorded.

5.5.4 Alarm-Response Internal Investigation. A SAP-indoctrinated individual shall arrive within 60 minutes to conduct an internal inspection of the SAPF, attempt to determine the probable cause of the alarm activation, and reset the IDS prior to the departure of the response force.

5.5.5 IDS Catastrophic Failure Coverage. In the case of IDS failure, SAP-indoctrinated personnel shall provide security by physically occupying the SAPF until the IDS returns to normal operation. As an alternative, the outside SAPF perimeter shall be continuously protected by the response force or a guard force until the SAPF can be continuously manned by SAP-indoctrinated personnel. A catastrophic failure plan shall be incorporated into the SAPF SOP submitted in writing to the PSO for review and approval prior to implementation. (See paragraph 6.1.2.)

6.0 Documentation Requirements. The following documentation shall be developed for the IDS. This documentation shall be made available to the PSO on request and shall be available within the SAPF.

6.1 Plans, Agreements, and Standard Operating Procedures (SOP)

6.1.1 IDS Plans. The IDS design and installation documentation shall be provided to the government sponsoring activity and maintained in the SAPF as specified in paragraph 3.1.4.

6.1.2 Catastrophic Failure Plan. If an alternative catastrophic failure plan is contemplated (see paragraph 3.1.3), the plan shall be submitted in writing to the PSO for review and approval prior to implementation.



6.1.3 Support Agreement. A written support agreement shall be established for external monitoring, response, or both. The agreement shall include the response time for both response force and SAPF personnel, responsibilities of the response force upon arrival, maintenance of SAPF points of contact, and length of time response personnel are required to remain on-site.

6.1.4 Monitoring Operator SOP. The duties of the monitor operator shall be documented in a SOP. The SOP shall include procedures for observing monitor panel(s) for reports of alarms, changes in IDE status, assessing these reports, and in the event of an intrusion alarm, dispatching the response force or notifying the proper authority to do so and notifying the appropriate authority of the event. [Note: These procedures shall state that the operator will not have any additional duties that may interfere with monitoring alarms, making assessments, and dispatching the response force.]

6.1.5 Maintenance Access SOP. A written SOP shall be established to address the appropriate actions to be taken when maintenance access is indicated at the monitor-station panel. The SOP shall require that all maintenance periods shall be archived in the system.

6.2 Records, Logs, and Archives

6.2.1 Test Records. A record of IDE testing shall be maintained within the SAPF. This record shall include: testing dates, names of individuals performing the test, specific equipment tested, malfunctions detected, and corrective actions taken. Records of the response-force personnel testing shall also be retained. All records of testing shall be maintained for a minimum of two years. (See paragraph 5.2.2.)

6.2.2 IDS Event (Alarm) Log. If the IDS has no provision for automatic entry into archive (see paragraph 3.2.6), the operator shall record the time, source, type of alarm, and action taken. The

responsible SAPF security officer shall routinely review the historical record. Results of investigations and observations by the response force shall also be maintained at the monitoring station. The SAPF security officer shall routinely review the historical record. Records of alarm annunciations shall be retained for a minimum of two years and longer if needed until investigations of system violations and incidents have been successfully resolved and recorded.

6.2.3 Annunciation of Shunting or Masking Condition Log. Shunting or masking of any zone or sensor shall be appropriately logged or recorded in an archive. (See paragraph 3.2.10.3.)

6.2.4 Maintenance Period Archives. All maintenance periods shall be archived into the system. (See paragraph 3.2.10.3.)

6.2.5 Remote Service Mode Archive. An archive shall be maintained for all remote service mode activities. (See paragraph 3.2.10.4.)

6.3 SAPF Accreditation File. IDS accreditation documentation shall be maintained on-site in the SAPF accreditation file. The following documents shall be included in the SAPF accreditation file along with other SAPF accreditation documentation: Final acceptance tests of original installation and any modifications; catastrophic failure plan (see paragraph 6.1.2); monitoring operator SOP (see paragraph 6.1.5); maintenance mode and remote service mode archives (see paragraphs 6.2.3 through 6.2.5); and, historical record of IDS logging (see paragraph 6.2.2). Final acceptance tests and the catastrophic failure plan shall be maintained in both the SAPF accreditation file and at the PSO location.



JOINT AIR FORCE - ARMY - NAVY (JAFAN) MANUAL 6/9

Annex C - Acoustical Control and Sound Masking Techniques

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

1.1 The STC Rating: STC is a single number rating used to determine the sound barrier performance of walls, ceilings, floors, windows, and doors.

1.2 Use of Sound Groups: The current edition of Architectural Graphics Standards (AGS) describes various types of sound control, isolation requirements and office planning. The AGS established Sound Groups I through 4, of which Groups 3 and 4 are considered adequate for specific acoustical security requirements for SAPF construction.

1.2.1 Sound Group I - STC of 30 or better. Loud speech can be understood fairly well. Normal speech cannot be easily understood.

1.2.2 Sound Group 2 - STC of 40 or better. Loud speech can be heard, but is hardly intelligible. Normal speech can be heard only faintly if at all.

1.2.3 Sound Group 3 - STC of 45 or better. Loud speech can be faintly heard but not understood. Normal speech is unintelligible.

1.2.4 Sound Group 4 - STC of 50 or better. Very loud sounds, such as loud singing, brass musical instruments or a radio at full volume, can be heard only faintly or not at all.

2. Sound Reduction for SAPFs. The amount of sound energy reduction may vary according to individual facility requirements. However, Sound Group ratings shall be used to describe the effectiveness of SAPF acoustical

security measures afforded by various wall materials and other building components.

2.1 All SAPF perimeter walls shall meet Sound Group 3, unless additional protection is required for amplified sound.

2.2 If compartmentation is required within the SAPF, the dividing office walls must meet Sound Group 3.

3. Sound Masking and Stand-Off Distance

3.1 When normal construction and baffling measures have been determined to be inadequate for meeting Sound Group 3 or 4, as appropriate, sound masking shall be employed. Protection against interception of SAP discussions may include use of sound masking devices, structural enhancements, or SAPF perimeter placement.

3.1.1 Sound masking devices may include vibration and noise generating systems located on the perimeter of the SAPF.

3.1.2 Structural enhancements may include the use of high density building materials (i.e. sound-deadening materials) to increase the resistance of the perimeter to vibration at audio frequencies.

3.1.3 SAPF perimeter placement may include construction design of a stand-off distance between the closest point a non-SAP-indoctrinated person could be positioned and the point where SAP discussions become available for interception. Use of a perimeter fence or protective zone between the SAPF perimeter walls and the closest "listening place" is permitted as an alternative to other sound protection measures.

3.2 Masking of sound which emanates from a SAP discussion area is commonly done by a sound masking system. A sound masking system may utilize a noise generator, tape, disc or record player as a noise source and an amplifier and speakers or transducers for distribution.



4. Placement of Speakers and

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

4.1 For common walls, the speakers/transducers should be placed so the sound optimizes acoustical protection.

4.2 For doors and windows, the speakers/transducers should be close to the aperture of the window or door and the sound projected in a direction facing away from conversations.

4.3 Once the speakers or transducers are optimally placed, the system volume must be set and fixed. The level for each speaker should be determined by listening to conversations occurring within the SAPF and the masking sound and adjusting the volume level until conversations are unintelligible from outside the SAPF.

5. Installation of Equipment

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

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

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

6.1 Audio amplifier with a record turntable.

6.2 Audio amplifier with a cassette, reel-to-reel, Compact Disc (CD), or Digital Audio Tape (DAT) playback unit.

6.3 Integrated amplifier and playback unit incorporating any of the above music sources.

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

7.1 All incoming wiring shall breach the SAPF perimeter at one point. TEMPEST or TSCM concerns may require electronic isolation.

7.2 In systems that require notification only, the system shall have a high gain buffer amplifier. In systems that require two-way communication, the system shall have electronic isolation. SAPF occupants should be alerted when the system is activated. All electronic isolation components shall be installed within the SAPF as near to the point of SAPF egress as possible.



JOINT AIR FORCE - ARMY - NAVY (JAFAN) MANUAL 6/9

Annex D - Personnel Access Controls

1. General Requirements. All SAPFs shall have personnel access control systems to control access at all perimeter entrances. Placards, signs, notices, and similar items are not acceptable as personnel access control systems. Unless otherwise stated herein, SAPF entrances shall be under visual control to deny unauthorized access unless the SAPF is unoccupied and secured. Such visual control may be accomplished by employees, guards using closed circuit television (CCTV), or other similar and approved methods. If CCTV is used for providing visual control, the CCTV equipment shall be continuously monitored by appropriately SAP-indoctrinated personnel. Personnel access control systems as specified herein do not replace or modify any requirement to properly secure SAPF doors as specified in JAFAN 6/9.

2. Automated Access Control Systems. Automated personnel access control systems meeting the following criteria may be used to control admittance to SAPFs during working hours in lieu of visual control.

2.1 Identification Requirement. The automated personnel access control system shall verify the identity of an individual by one of the following methods:

2.1.1 Identification (ID) Badges or Cards. The ID badge or card must identify to the access control system the individual to whom the card is issued. A personal identification number (PIN) is required. The PIN must be separately entered into the system by each individual using a keypad device and shall consist of four or more digits, randomly selected, with no known or logical association with the individual.

2.1.2 Personal Identity Verification. Personal identity verification (biometrics device) identifies the individual requesting access by some unique personal characteristic.

2.2 Authentication Requirement. The automated personnel access control system shall authenticate an individual's authorization to enter

the SAPF by matching the applicable information specified in the previous paragraph with personnel data contained in an automated database to authenticate the individual's authorization prior to giving the individual access to the SAPF.

2.3 Accept/Reject Threshold Criteria. Automated personnel access control equipment or devices shall meet the following criteria during normal equipment operation: The probability of an unauthorized individual gaining access is no more than one in ten thousand while the probability of an authorized individual being rejected access is no more than one in one thousand. Prior to using such equipment, manufacturers must certify in writing that their equipment conforms to this criterion.

2.4 System Protection. Physical security protection must be established and continuously maintained for all devices/equipment that comprise the personnel access control system. The level of protection may vary depending upon the type of devices/equipment being protected. Existing security controls within the facility shall be used to the extent practical in meeting this requirement.

2.5 Transmission Line Protection. System data that is carried on transmission lines (e.g., access authorizations, personal identification, or verification data) to and from devices/equipment located outside the SAPF shall be encrypted with an approved 128-bit, or greater, encryption algorithm. The algorithm must be certified by NIST or another US government authorized independent testing laboratory. If the communication technology described above is not feasible, the transmission line will be installed within a protective covering to preclude surreptitious manipulation, or be adequately supervised to protect against modification and/or substitution of the transmitted signal.

2.6 Door Strikes. Electric door strikes installed for use in personnel access control systems shall be heavy-duty industrial grade.

2.7 Personnel and System Data Protection. Locations where authorization data, card-encoded data, and personal identification or verification data is input, stored, or recorded must be protected within



a SAPF or an alarmed area controlled at the SECRET level. Records and information concerning encoded ID data, PINs, authentication data, operating system software, or any identifying data associated with the personnel access control system shall be kept secured when unattended. Access to the data shall be restricted. (See paragraph 4.3.)

2.8 External Devices. Card readers, keypads, communication, or interface devices located outside the entrance to a SAPF shall have tamper resistant enclosures and be securely fastened to a wall or other structure.

2.9 Electrical components, associated wiring, or mechanical links (cables, rods, and so on) should be accessible only from inside the SAPF, or if they transverse an uncontrolled area they shall be secured within a protective covering to preclude surreptitious manipulation of components.

2.10 Records shall be maintained to reflect the current active assignment of ID badge/card, PIN, level of access, entries, and similar system-related elements. Records concerning personnel removed from the system shall be retained for a minimum of two years. Records of entries to SAPFs shall be retained for a minimum of two years. Records concerning investigations of system violations and incidents shall be retained until they have been successfully resolved and recorded.

3. Non-Automated Access Control. Non-automated access control (electric, mechanical, or electromechanical) that meet the criteria stated below may be used to control admittance to SAP areas during working hours if the entrance is under visual control (see paragraph 1.0). These systems are also acceptable to control access to compartmented areas within the SAPF. Non-automated access system devices must be installed in the following manner:

3.1 Control Panel Location and Shielding. The control panel in which the combination and all associated cabling and wiring is set shall be located inside the SAPF and will require minimal physical security designed to deny unauthorized access to its mechanism. The control panel shall be installed, or have a shielding device mounted such that an unauthorized person in the immediate vicinity cannot observe the setting or changing of the combination. (See paragraph 4.4.)

3.2 Access Code Protection. Keypad and cypher devices shall be designed or installed in such a manner that unauthorized individuals in the immediate vicinity cannot observe the entry of the access code.

4. Personnel Requirements and

Restrictions. Operating personnel access control systems in accordance with this Annex requires that the below personnel requirements and restrictions be followed:

4.1 Entering and Leaving a SAPF. Personnel entering or leaving a SAPF are required to ensure the entrance or exit point is properly closed. Authorized personnel who permit another individual to enter the area are responsible for confirming the individual's access and need-to-know.

4.2 Escorting. A resident SAP-indoctrinated person who is knowledgeable of the security procedures of the SAPF shall continuously escort persons within the SAPF who are not issued a "NO ESCORT REQUIRED" visitor's badge.

4.3 Access to Personnel and System Data. Access to records and information concerning encoded ID data and PINs shall be restricted to authorized SAP-indoctrinated personnel. Access to identification or authentication data, operating system software, or any identifying data associated with the personnel access control system shall be limited to the least number of personnel possible.

4.4 Setting Combinations. The selection and setting of the combination shall be accomplished by SAP-indoctrinated individuals. The combination shall be changed upon initial installation and when compromised or an individual knowledgeable of the combination no longer requires access.

4.5 System Records Maintenance. A procedure shall be established for removing an individual's authorization to enter an area when the individual is transferred, terminated, or the individual's access is suspended, revoked, or downgraded to a level below that required for entry. Compromised access cards and/or PINs will be immediately reported and removed from the system.



JOINT AIR FORCE - ARMY - NAVY (JAFAN) MANUAL 6/9

Annex E - Telecommunications Systems and Equipment

This Annex establishes a baseline requirement for the protection of sensitive information within Special Access Program Facilities (SAPFs) from intrusion and exploitation via unclassified telecommunications systems, devices, equipment, software, and features. Compliance with these standards is mandatory for all SAPFs and/or systems established after the effective date of this Annex.

1. Applicability and Scope. The telecommunications security measures of this Annex apply to the planning, installation, maintenance, and management of telecommunication systems and equipment within SAPFs, in both foreign and domestic locations. The security measures of this Annex apply to any telecommunication system that provides service to a SAPF. The requirements contained in this Annex are designed to prevent inadvertent disclosure or loss of sensitive, intelligence bearing, and compartmented information through telecommunication systems and to protect against the clandestine exploitation and/or disruption of SAPF operations through these systems. This Annex is compatible with but may not satisfy requirements of other security disciplines such as COMSEC, OPSEC, or TEMPEST.

2. Requirements. At a minimum, the following requirements must be met to ensure proper safeguards for the protection of information: configuration of telecommunications systems, devices, features, and software; access control; and control of the cable infrastructure. The audio protection requirements of this Annex do not apply if the SAPF is declared a "No Classified Discussion Area" and warning notices are posted prominently within the SAPF.

2.1 Baseline Configuration

2.1.1 A baseline configuration of all telecommunications systems, devices, features, and software must be established, documented, and included in the Fixed Facility Checklist (JAFAN 6/9 Annex A) or as an attachment.

2.1.2 The Program Security Officer (PSO) will review the telecommunications system baseline configuration and supporting/supplementing information to determine if the risk of information loss or exploitation has been suitably mitigated. When the following requirements are unachievable, the associated telecommunications equipment must be

installed and maintained in non-discussion areas or a written waiver must be issued by the PSO.

2.2 Unclassified Telecommunications Systems. Unclassified telecommunications systems in SAPFs shall not pass/transmit sensitive audio discussions when they are idle and not in use. Additionally, these telecommunications systems shall be configured to prevent external control or activation. The concepts of "on-hook" and "off-hook" audio protection⁴ outlined in telephone security group (TSG) standards 2 and 6 must be incorporated into SAPF telecommunications systems.

2.2.1 Unclassified telephone systems and services shall be configured to prevent technical exploitation or penetration. In addition, these systems shall incorporate physical and software access controls to prevent disclosure or manipulation of system programming and stored data. The PSO must ensure that the following specific requirements are applied to unclassified telecommunications systems:

2.2.1.1 Provide on-hook audio protection by the use of TSG 6 instrument(s), TSG 6-approved disconnect devices, or equivalent TSG 2 system configuration.

2.2.1.2 Provide off-hook audio protection by use of a hold feature, modified handset (push-to-talk), or equivalent.

2.2.1.3 Provide isolation by use of a computerized telephone system (CTS) with software and hardware configuration control and control of audit reports (such as station message detail reporting, call detail reporting, etc.). System programming will not include the ability to place, or keep, a handset off-hook.

⁴ On-hook audio protection is the assurance that a telephonic device does not pick-up and process audio when the phone is hung-up and considered to be idle. Off-hook audio protection is the assurance that when the phone is in use, but temporarily unattended, that near-by audio is not picked up and processed through the use of a "hold feature" or a push-to-talk handset.



Configuration of the system must ensure that all on-hook and off-hook vulnerabilities are identified and mitigated.

2.2.1.4 Ensure that equipment used for administration of telephone systems is installed inside an area where access is limited to authorized personnel. When local or remote administration terminals (for a CTS) are not or cannot be contained within the controlled area, and safeguarded against unauthorized manipulation, then the use of TSG 6-approved telephone instruments shall be required, regardless of the CTS configuration.

2.2.1.5 Ensure that remote maintenance, if used, is protected against manipulation/activation by means of a dial-back modem, network boundary security device (firewall), or other appropriate device.

2.2.1.6 Ensure that speakerphones and audio conferencing systems are not used on unclassified telecommunications systems in SAPFs. Exceptions to this requirement may be approved by the PSO, when these systems have sufficient audio isolation from other classified discussion areas in the SAPF, and procedures are established to prevent inadvertent transmission of classified information.

2.2.1.7 Ensure that features used for voice mail or unified messaging services are configured to prevent unauthorized access to remote diagnostic ports or internal dial tone.

2.2.1.8 Ensure that telephone answering devices (TAD) and facsimile machines do not contain features that introduce security vulnerabilities, e.g., remote room monitoring, remote programming, or other similar features that may permit off-premise access to room audio. Prior PSO approval is required before installation or use.

2.2.2 All unclassified telecommunications systems and associated infrastructure must be electrically and physically isolated from any classified information/telecommunications systems in accordance with National Security Telecommunications and Information Systems Security Committee requirements or any other separation standards applied to the classified information system on site.

2.3 Unclassified Information Systems. Unclassified information systems must be safeguarded to prevent manipulation of features and software that could result in the loss/compromise of sensitive audio information or protected data.

2.3.1 Ensure that all computer/telecommunications equipment with telephonic or audio features are protected against remote activation and/or exfiltration of audio information over any connections (i.e., disconnecting the microphone, inserting a blank plug in the microphone jack, etc.).

2.3.2 Ensure that all video cameras used for unclassified video teleconferencing and/or video recording equipment are deactivated and disconnected when not in use. In addition, video devices used in SAPFs must feature a clearly visible indicator to alert SAPF personnel when recording or transmitting.

2.4 Environmental Infrastructure Systems.

Environmental infrastructure systems are the basic human comfort, security, and life safety systems that support SAPF operations. Advancements in technology have created conditions whereby many of these amenities are computer-automated with public switched telephone network or other connections for remote monitoring, access, and external control/manipulation of features and services. Fixed facility checklists (FFC) will identify any such connection to environmental systems within SAPFs, and document measures taken to provide protection against malicious activity, intrusion, and exploitation. Protection mechanisms and current configurations for infrastructure systems, such as premise management systems, environmental control systems, lighting and power control units, uninterrupted power sources, and such, which provide services to the SAPF, shall be included in the SAPF baseline evaluation (whether or not they reside in the SAPF).

2.5 Wireless Technology. The use of any device, or system utilizing wireless technology must be approved by the PSO prior to purchase and introduction into the SAPF. All TEMPEST/Technical Security concerns shall be weighed against the facilities overall security posture (i.e., facility location, threat, as well as any compensatory countermeasures that create a “security in-depth” concept) when evaluating these wireless systems. All separation and isolation standards provided in NSTISSC standards are applicable to unclassified wireless systems installed or used in SAPFs.

2.6 Access Control. Installation and maintenance of unclassified telecommunications systems and devices supporting SAPF operations may require physical and/or electronic access. Remote maintenance may be performed as described in paragraph 2.6.2. Under other circumstances, physical access may be required to perform computer-based diagnostics to make necessary repairs. Therefore, the following paragraphs identify



the minimum requirements for providing access to unclassified telecommunications systems and devices supporting SAPF operations. These requirements are applicable regardless of whether or not the telecommunications device resides within the SAPF or is contained in a protected area outside the SAPF, so long as it is deemed as a critical infrastructure item by the PSO.

2.6.1 Physical Access Control. Installation and maintenance personnel will possess an appropriate clearance and access or will be continuously escorted and monitored by technically knowledgeable SAP-cleared and -accessed personnel at all times within the SAPF. Furthermore, physical access to telecommunications equipment shall be limited to prevent unauthorized modifications or reconfiguration.

2.6.2 Remote Maintenance and Diagnostic Access. All capabilities for remote maintenance and diagnostic services must be clearly specified in the Fixed Facility Checklist (FFC.) The FFC will include all procedures and countermeasures preventing unauthorized system access, unauthorized system modification, or introduction of unauthorized software as specified in TSG 2 paragraph 4d.

2.6.2.1 Remote maintenance and diagnosis may be performed from a secure facility over a protected link (i.e., dial-back or DES modem).

2.6.2.2 Failing the steps outlined in paragraph 2.6.2.1, remote maintenance and diagnosis may be performed over an unclassified telephone line as specified in TSG 2 paragraph 4c.

2.7 Memory and Storage Media. Any telecommunication system, component and/or like devices with memory or digital storage capabilities, to include multi-function devices, (i.e., facsimile, printers, copiers, scanners, etc.) will be sanitized of any sensitive information before being repaired or released to unclassified personnel.

2.7.1 The baseline configuration document, FFC, will identify all memory and data storage systems of all unclassified telecommunications systems that contain sensitive data or information that is of concern for operational security purposes. This storage media will be sanitized before it is removed from the facility for any purpose, including maintenance or disposal. Similarly, this storage media will not be made available to unclassified technicians or maintenance personnel.

2.7.2 Storage media that cannot be effectively sanitized will be removed from the telecommunications system prior to repair or disposal, and be destroyed by approved methods.

2.8 SAPF Cable Control

2.8.1 All unclassified telecommunications cabling⁵ should enter the SAPF through a common opening. The cables should be installed in a professional manner such that they can be visually inspected without difficulty.

2.8.2 Each conductor (fiber or metallic) should be accurately accounted for from the point of entry. The accountability should identify the precise use of every conductor through labeling, log, or journal entries. Spare conductors will be identified and appropriately grounded.

2.8.3 Unused conductors will be removed. If removal is not feasible, the PSO may require the metallic conductors to be stripped, bound together, and grounded at the point of ingress/egress. Unused fiber conductors will be uncoupled from the interface within the SAPF, capped, and labeled as unused.

3. Responsibilities

3.1 NTSWG. The National Telecommunications Security Working Group (NTSWG) is responsible for developing security countermeasure solutions for unclassified telecommunications systems and devices.

3.2 PSO. The PSO is responsible for selecting, implementing, and verifying security measures to balance the vulnerabilities of the telecommunications system(s) against technical threats of its environment. This requires the PSO to:

3.2.1 Know this Annex and be able to assist site security personnel with implementation.

3.2.2 Review the FFC and certify that all the requirements of this Annex have been met. When the requirements of this Annex cannot be met, the PSO must mitigate the risk through the application of countermeasures or waive the requirement.

3.2.3 Assist site security personnel in selecting telecommunications equipment and/or recommending appropriate countermeasures.

⁵ Telecommunications cabling includes all cables used to support SAPF operations, to include wiring for fire annunciation and evacuation systems which may only run throughout the building, but may not connect to the PSTN.



3.2.4 Maintain a current set of reference documents as listed in section 4.0 below.

3.2.5 Responsible for ensuring that a full risk assessment is performed prior to issuance of a waiver or exception to the provisions of this document, and for ensuring that any waiver or exception is periodically reviewed. Any such waivers or exceptions must be documented.

3.2.6 Request technical surveillance countermeasure (TSCM) inspections, as conditions warrant, to prevent the loss or compromise of protected information through the intrusion and exploitation of a telecommunications system in accordance with DCID 6/2.

3.3 Site Security Personnel. The site security personnel are responsible for implementing the requirements of this Annex and requesting PSO approval for new telecommunications systems, devices, features, hardware, and major modifications to existing systems by:

3.3.1 Submitting necessary documentation on new systems and/or modified systems and recommending security countermeasures and options to the PSO as appropriate.

3.3.2 Maintaining a record set of documentation on site.

3.3.3 Adhering to the guidance set forth by the PSO.

3.3.4 Notifying the PSO of any suspected or actual attempts to intrude or exploit a telecommunications or infrastructure system supporting SAPF operations. When warranted, site security personnel will assist the PSO with investigating and resolving incidents and applying additional countermeasures as required.

3.3.5 Determining that telecommunications systems and devices are properly sanitized or cleared prior to any maintenance procedures, and that all networked interconnections are removed (isolated) during maintenance routines.

3.3.6 Authorizing diagnostics connections (either remote or on-site) for the purpose of performing maintenance on telecommunications systems and devices, and conducting reviews of on-site test data prior to releasing it from the protected area.

4. References

4.1 NTSWG (formerly known as the TSG). Standards and information series that refer to the published guidance provided by the NTSWG for the protection of sensitive information and unclassified telecommunications information processing systems and equipment. The following documents are intended for use by all personnel concerned with telecommunications security.

4.1.1 TSG Standard 1, (*Introduction to Telephone Security*). Provides telephone security background and TSG-approved options for telephone installations in US Government sensitive discussion areas.

4.1.2 TSG Standard 2 (*TSG Guidelines for Computerized Telephone Systems*) and its Annexes. Establishes requirements for planning, installing, maintaining, and managing a CTS, and provides guidance for personnel involved in writing contract, inspecting, and system administration of a CTS.

4.1.3 TSG Standard 6, (*TSG-Approved Equipment*). Lists TSG-approved equipment which inherently provides protection against the accidental collection and conduction of information from within sensitive discussion areas.

4.1.4 TSG Standards 3,4,5,7, and 8. Contains design specifications for telecommunication manufacturers. (*Not necessarily applicable to facility security personnel.*)

4.1.5 Information Series (*Computerized Telephone Systems (CTSs) A Review of Deficiencies, Threats, and Risks*, dated: December 1994). Describes deficiencies, threats, and risks associated with computerized telephone systems which impact the loss of "on-hook" audio, as well as the protection of unclassified information stored/contained within the CTS and its telephone devices.

4.1.6 Information Series (*Executive Overview*, dated: October 1996). Provides the salient points of the TSG standards and presents them in a non-technical format.

4.1.7 Information Series (*Central Office (CO) Interfaces*, dated: November 1997). Provides an understanding of the types of services delivered by the local central office and describes how they are connected to administrative telecommunications systems and devices.

4.1.8 Information Series (*Everything You Always Wanted to Know about Telephone Security...but were*



afraid to ask, second edition, dated: December 1998). Distills the essence of the TSG standards (which contain sound telecommunications practices) and presents them in a readable, non-technical manner.

4.1.9 Information Series (*Infrastructure Surety Program...securing the last mile*, dated: April 1999). Provides a basic understanding of how to protect office automation and infrastructure systems that contribute to successful mission accomplishment.

4.1.10 Information Series (*Computerized Telephone Systems Security Plan Manual*, dated: May 1999). Assists in implementing and maintaining the “secure” operation of CTSs when used to support SAPF operations. The term “secure” relates to the safe and risk-free operation, not the use of encryption or a transmission security device.

4.2 Director of Central Intelligence Directive (DCID 6/3). (*Protecting Sensitive Compartmented Information Within Information Systems*.)

4.3 SPB Issuance 00-2 (18 January 2000). Infrastructure Surety Program (ISP) and the Management Assessment Tool (MAT).

5. Definitions

5.1 Critical Infrastructure Item. Any component or group of components that provide essential functions or support to the SAPF operation, or that is relied upon as an isolation component/device to assure that SAPF-based telecommunications cannot be electronically accessed to exploit information. Examples include: uninterrupted power sources (UPS); computerized telephone system (CTS); and/or energy management systems (EMS); which provide power, telephone, lighting, and HVAC for the SAPF (which often reside outside the SAPF perimeter).

5.2 Environmental Infrastructure Systems. Those systems and devices that provide critical support to the SAPF in which sensitive/SAP information processing takes place. The denial or degradation of environmental/infrastructure systems will have a cascading effect on the denial or degradation of information processing and information availability. Therefore, this Annex will address the minimum protection necessary to ensure a continuity of service to thwart the effects of denial of service attacks or external manipulation of environmental/infrastructure systems.

5.3 Sensitive/SAP Information. Information requiring enhanced security safeguards per US

Government directives for information such as: classified national security information (CNSI), Special Access Program (SAP) information, sensitive compartmented information (SCI), restricted data (RD), sensitive but unclassified (SBU) information, and For Official Use Only (FOUO).

5.4 Site Security Personnel. Individual(s) responsible for SAPF security, including physical and technical security, and information protection. This term is synonymous with the Program Security Officer (PSO), Information Systems Security Representative (ISSR), Command/Contractor Program Security Officer (CPSO), Facility Security Officer (FSO), Facility Security Manager (FSM), and others which may be agency specific terms.

5.5 Wireless. Any communications path or method that does not rely totally on a copper wire or fiber for its transmission medium, i.e., infra-red (IR), radio frequency (RF), etc.

5.6 Computerized Telephone System (CTS). A generic term used to describe any telephone systems that use centralized stored program computer technology to provide switched telephone networking features and services. CTSs are referred to commercially by such terms as computerized private branch exchange (CPBX), private branch exchange (PBX), private automatic branch exchange (PABX), electronic private automatic branch exchange (EPABX), computerized branch exchange (CBX), computerized key telephone system (CKTS), hybrid key systems, business communications systems, and office communications systems.



9 December 2004

CHANGE ONE to JAFAN 6/9

The following modifications to Annex B, "*Intrusion Detection Systems (IDS)*" to the Joint Air Force-Army-Navy (JAFAN 6/9) Manual, "*Physical Security Standards for Special Access Program Facilities*" dated 23 March 2004 have been approved. Please make the following pen-and-ink changes:

Paragraph 3.1.1, Page 34. **Replace first sentence to read:**

"All areas of a SAPF that reasonably afford access to the SAPF, or where SAP is stored, shall be protected by an IDS, unless continuously occupied."

Paragraph 3.1.5, Page 34. **Replace last sentence to read:**

"ISA comprised of IDE with auto-reset features may be used with the concurrence of the PSO."

Paragraph 3.2.7, Page 36. **Change paragraph to read:**

"All alarm activations shall be reset using designated personnel unless the auto reset feature has been approved by the PSO."

Paragraph 5.3.1, Page 39. **Change paragraph to read:**

"The IDE shall be maintained by US citizens. Non-US citizens shall not provide these services without prior written approval by the PSO."

When the above pen-and-ink changes have been made, annotate at the top of the front cover that "Change One to Annex B incorporated on (d a t e)" and insert this change transmittal sheet as the last page of JAFAN 6/9.

PAUL HARALDSEN
Director of SAP Security
Office of the Director, Security
and Special Programs Oversight

SCOTT MAGNINO
Director of SAP Security
Office of the Director,
Technology Management
Office (TMO)

DANIEL GRAGG
Director of SAP Security
Office of the Director,
Special Programs
Office (CNO (N7SP))

AIR FORCE

ARMY

NAVY