Department of Defense
MANUAL

NUMBER 5205.07, Volume 3
April 23, 2015
Incorporating Change 3, Effective December 8, 2020

USD(I&S)

SUBJECT: DoD Special Access Program (SAP) Security Manual: Physical Security

References: See Enclosure 1

1. PURPOSE

a. Manual. This manual is composed of several volumes, each containing its own purpose. The purpose of the overall manual, in accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), is to implement policy established in DoDD 5205.07 (Reference (b)), assign responsibilities, and provide security procedures for DoD SAP information.

b. Volume. This volume:

(1) Implements policy established in DoD Instruction (DoDI) 5205.11 (Reference (c).

(2) Assigns responsibilities and provides procedures for physical security for DoD SAPs.

2. APPLICABILITY

a. This volume applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this volume as the "DoD Components").

(2) All DoD Component contractors and consultants that require access to DoD SAPs pursuant to the terms and conditions of the contract or agreement.

(3) Non-DoD U.S. Government departments, activities, agencies, and all other organizational entities that require access to DoD SAPs pursuant to the terms and conditions of a memorandum of agreement or other interagency agreement established with the DoD.

b. Nothing in this volume will be construed to contradict or inhibit compliance with chapter 126 of Title 42, United States Code (Reference (d)) or building codes.

3. POLICY. It is DoD policy in accordance with Reference (b) that DoD SAPs be established and maintained when absolutely necessary to protect the most sensitive DoD capabilities, information, technologies, and operations or when required by statute.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES

a. All applicable DoD Components and entities specified in paragraph 2a will follow Reference (b), the general procedures in this volume, and the standards and processing procedures and templates on the Defense Security Service (DSS) Website (http://www.dss.mil/isp/specialprograms.html). See Enclosure 3 concerning the physical standards for protecting SAP information.

b. SAP-accredited areas that are presently accredited, under construction, or in the approval process at the effective date of this volume will not require modification to conform to these standards. SAP-accredited areas undergoing major modification may be required to comply entirely with the provisions of this volume. Approval for such modifications will be requested and approved in accordance with Enclosure 3 of this volume.

6. RELEASABILITY. **Cleared for public release**. This volume is available on the Directives Division website at https://www.esd.whs.mil/DD/.

7. SUMMARY OF CHANGE 3. This administrative change:

a. Updates the title of the Under Secretary of Defense for Intelligence to the Under Secretary of Defense for Intelligence and Security in accordance with Public Law 116-92 (Reference (e)).

b. Updates references.

8. EFFECTIVE DATE. This volume is effective April 23, 2015.

Michael G. Vickers
Under Secretary of Defense for Intelligence

Enclosures
1. References
2. Responsibilities
3. General Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended
(b) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended
(c) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," February 6, 2013, as amended
(d) Chapter 126 of Title 42, United States Code
(e) Public Law 116-92, "National Defense Authorization Act for Fiscal Year 2020," December 20, 2019
(f) Office of the National Counterintelligence Executive, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities, Version 1.2," April 23, 2012
(g) Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities," May 26, 2010
(h) DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM)," April 3, 2014, as amended
(i) DoD Manual 5105.21, Volume 2, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Physical Security, Visitor Control, and Technical Security," October 19, 2012, as amended
(j) Federal Specification FF-L 2740B, "Locks, Combination, Electromechanical," June 15, 2011[1]
(k) Committee on National Security Systems Instruction 7000, "TEMPEST Countermeasures for Facilities," May 2004[2]
(l) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(m) Committee on National Security Systems Advisory Memorandum TEMPEST/01-13, "Red/Black Installation Guidance," January 17, 2014[3]

[1] View at NIPRNET http://www.gsa.gov/portal/content/103856#FederalSpecifications
[2] View at SIPRNET at http://www.iad.nsa.smil.mil/resources/library/cnss_section/cnss_instructions.cfm
[3] View at SIPRNET at http://www.iad.nsa.smil.mil/resources/library/cnss_section/pdf/TEMPEST_CNAS SAM_01_13.pdf

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S) develops and maintains this volume.

2. DIRECTOR, DSS. Under the authority, direction, and control of the USD(I&S), the Director, DSS, conducts security oversight functions to validate the certification and accreditation of industrial special access program facilities (SAPFs) in accordance with Reference (c).

3. DIRECTOR, DoD SPECIAL ACCESS PROGRAM CENTRAL OFFICE (SAPCO). Under the authority, direction, and control of the Deputy Secretary of Defense, the Director, DoD SAPCO, verifies that the physical security measures implemented by the congressional committees processing and storing DoD SAP information meet the standards of this volume.

4. DoD COMPONENT HEADS AND OSD PRINCIPAL STAFF ASSISTANTS (PSAs) WITH COGNIZANT AUTHORITY (CA) AND OVERSIGHT AUTHORITY (OA) OVER SAPs. The DoD Component heads and OSD PSAs with CA and OA over SAPs implement the procedures in this volume.

5. DIRECTORS OF THE DoD COMPONENT SAPCOs AND DIRECTORS OF THE PSA SAPCOs WITH CA AND OA OVER SAPs. Directors of the DoD Component SAPCOs and Directors of the PSA SAPCOs with CA and OA over SAPs:

a. Establish training standards for and designate properly trained special access program facility accrediting officials (SAOs).

b. Grant waivers to the standards stipulated in this volume based on a risk assessment and operational requirements.

ENCLOSURE 3

GENERAL PROCEDURES

1. GENERAL

a. The procedures in this enclosure are minimum standards for providing physical security in the DoD Components. It is at the discretion of the DoD Components to provide more specific guidance.

b. A SAPF, temporary special access program facility (T-SAPF), special access program compartmented area (SAPCA), special access program working area (SAPWA), or special access program temporary secure working area (SAPTSWA) will be accredited by a CA SAPCO designated SAO before receiving, generating, processing, using, or storing SAP classified information, as appropriate to the accreditation.

(1) The government SAP security officer (GSSO) or the program security officer (PSO) and contractor program security officer (CPSO) responsible for the daily operation of the facility will notify the SAO of any activity that affects the accreditation. PSOs may perform SAO functions when designated by the CA SAPCO.

(2) The physical security safeguards established in the Office of the National Counterintelligence Executive Technical Specifications (Reference (f)) and Intelligence Community Directive 705 (Reference (g)) are the physical standards for protection of SAP information. Construction of SAPFs, T-SAPFs, SAPCAs¸ SAPWAs, and SAPTSWAs will conform to the equivalent sensitive compartmented information facility (SCIF), T-SCIF, CA, SWA, TSWA, as defined in Reference (f), unless variations are specifically noted in this volume.

c. Security standards will apply to all proposed SAP areas and will be coordinated with the SAO for guidance and approval. Location of construction or fabrication does not exclude a SAPF, T-SAPF, SAPCA, SAPWA or SAPTSWA from security standards and or review and approval by the SAO.

d. The Director, CA SAPCO must approve waivers for imposing safeguards exceeding a standard, even when the additional safeguards are based on risk.

e. When a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA are operational, only appropriately accessed SAP indoctrinated individual(s) will occupy them.

f. TEMPEST security measures must be considered if electronic processing will occur in the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA. The SAO will submit plans to a certified TEMPEST technical authority (CTTA) for assessment.

g. DoD contractors under the National Industrial Security Program will possess a facility security clearance (FCL) validated by the PSO and have an accredited SAPF, T-SAPF, SAPCA,

SAPWA, and SAPTSWA before receiving, generating, processing, using, or storing SAP classified information. The classification level of the SAP information within the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA cannot exceed the classification level of the FCL. The CPSO will notify the PSO of any activity that affects the FCL or SAP accreditation.

2. SAP-ACCREDITED AREAS. Areas where SAP material is processed, stored, discussed, manufactured, or tested may fall into one of these categories: SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA.

a. A SAPF (to include a T-SAPF) or SAPCA is an accredited area where SAP materials may be stored, used, discussed, manufactured, or electronically processed. SAPFs or SAPCAs may include fixed facilities, mobile platforms, and modular or prefabricated structures. Physical security protection for a SAPF or SAPCA will prevent as well as detect unauthorized visual, acoustical, technical, and physical access by unauthorized persons. Physical security criteria are governed by whether or not the SAPF or SAPCA is located in the United States and according to the operational criteria of closed storage, open storage, or continuous operations. Reference (f) details the specific construction, physical controls, and alarm systems for each situation.

b. A SAPCA is required when different compartmented programs are sharing the same SAPF and SCIF and not all personnel are cross-briefed. CA SAPCO designated SAO concurrence with visual, acoustic, and access control measures is required. Compartmented area personnel do not have to be briefed to the accreditation level of the parent SAPF or SCIF. However, appropriate operating procedures must be approved by the responsible PSO(s) or GSSOs that ensure separation of non-cleared personnel from the various SAPs operating in the SAPF or SCIF and the SAPCA. DoD SAPs will only be stored, used, discussed, manufactured, or electronically processed in Compartmented Area levels 2 or 3, as defined in Reference (g).

c. A SAPWA is an accredited area used for discussing, handling, or processing SAP. Storage of SAP material in a SAPWA is not authorized.

d. A SAPTSWA is an accredited area where handling, discussing, or processing of SAP is limited to less than 40 hours per month and the accreditation is limited to 12 months or less. Re-accreditation as a SAPTSWA requires a new physical inspection of the area. Storage of SAP material in a SAPTSWA is not authorized.

3. RISK MANAGEMENT

a. If, during a preconstruction and inspection phase, it is the determined that full compliance with the minimum standards contained in this volume is not possible, the SAO will select appropriate mitigating actions or activities based on analytical risk management process defined in Reference (f).

b. A determination made by the SAO that a facility's security SAP consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement

within the facility. Security in depth (SID) describes the factors that enhance the probability of detection before actual penetration to the SAPF. The existence of a layer or layers of security that offer mitigations for risks may be accepted by the SAO. An important factor in determining risk is whether layers of security already exist at the areas where SAP material is processed, stored, discussed, manufactured, or tested.

4. PHYSICAL SECURITY PRECONSTRUCTION REVIEW AND APPROVAL. SAOs will review physical security preconstruction plans for SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA construction, expansion, or modification to ensure compliance with applicable construction criteria standards in chapters 3 through 11 of Reference (f). Any proposed mitigation and SID will be documented in the plans. The approval or disapproval of a physical security preconstruction plan will be in writing and retained in the requester's files.

a. The requester will submit the appropriate checklist from Reference (f) for all SAP accreditations to the respective SAO for review and approval. The completed checklist will be classified in accordance with specific SAP security classification guidance.

b. The SAP fixed facility checklist (FFC) submission will include floor plans, diagrams of electrical and communications wiring; heating, ventilation, and air conditioning connections; security equipment layout (to include the location of intrusion detection equipment) and SID. All diagrams or drawings must be submitted on legible and reproducible media.

c. The SAPCA checklist should be accompanied by the FFC, associated floor plans, and current accreditation of the parent SAPF or SCIF with particular emphasis on the placement of intrusion detection system sensors, if required, and type of locks and access control used or proposed for the SAPCA.

5. SAP CONSTRUCTION PROCEDURES

a. The SAO will:

(1) Review and approve or disapprove the design concept, construction security plan (CSP), and final design for each construction project before the start of construction in accordance with Reference (f) and this volume.

(2) Physically inspect a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA before accreditation in accordance with construction standards in Reference (f) and this volume.

(3) Provide construction advice and guidance as required.

(4) Inspect SAPFs, T-SAPFs, SAPCAs, SAPWAs, and SAPTSWAs at an interval as determined by the CA SAPCO and withdraw accreditation when situations dictate.

(5) Approve and document mitigations commensurate with the standards in Reference (f).

(6) Recommend waivers of physical security safeguards to the Director, CA SAPCO.

(7) Ensure mitigating strategies are implemented and documented in the CSP in Reference (f) when using non-U.S. citizen workers.

(8) Request construction surveillance technicians to supplement site access controls, implement screening and inspection procedures, and monitor construction and personnel in accordance with Reference (f).

b. The site security manager will:

(1) Advise the SAO of the potential for variation from the requirements of this volume.

(2) In consultation with the SAO, develop a CSP regarding implementation of the standards of this volume and Reference (f). The CSP will include a plan of action and milestones required to document the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA construction from start to finish.

(3) Conduct periodic security inspections for the duration of the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA construction to ensure compliance with the CSP.

(4) Prepare necessary waiver requests and forward to the SAO for further processing.

(5) Investigate and document security violations or deviations from the CSP. Notify the PSO of security violations and the SAO of deviations from the CSP within 24 hours of incident detection

. (6) Implement physical access control measures in accordance with Reference (f).

c. CTTAs will:

(1) Review construction or renovation plans to determine if TEMPEST countermeasures are required and recommend solutions. To the maximum extent practicable, TEMPEST mitigation requirements will be incorporated into the design.

(2) Provide the SAO with documented results of the review with recommendations.

d. Construction security requirements are detailed in Reference (f) and Enclosure 3 of this volume.

6. ACCREDITATION

a. The procedures for establishment and accreditation of a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA will follow guidelines distributed by the CA SAPCO.

b. The SAO will inspect any SAP area before accreditation. Periodic re-inspections will be conducted based on threat, physical modifications, sensitivity of SAPs, and past security performance, but will be conducted no less frequently than every 3 years. Inspections, announced or unannounced, may occur at any time. The current FFC will be reviewed during inspections to ensure continued compliance. Technical surveillance countermeasures (TSCM) evaluations may be required at the discretion of the SAO, as conditions warrant, and will be implemented in accordance with DoDI 5240.05 (Reference (h)). Inspection reports will be retained within the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA and by the SAO. All SAPFs, T-SAPFs, SAPCAs, SAPWAs, and SAPTSWAs will maintain, on site, current copies of:

(1) SAP FFC and supporting documentation.

(2) Any accreditation documents (e.g., physical, TEMPEST, and information systems) and copies of any waivers granted by the CA SAPCO.

(3) SAPF accreditation approval documentation (including mitigations and waivers).

(4) TSCM reports, for the entire period of SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA accreditation.

(5) Operating procedures and any security documentation (including information system security authorization package, co-utilization agreements (CUAs), appointment letters, memorandums of agreement, and emergency action plans).

7. CO-UTILIZATION

a. DoD Components that want to co-utilize a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA will accept the current accreditation of the responsible agency if accredited without waiver to the standards in this volume. Prospective tenant activities will be informed of all mitigations and waivers to the requirements of this volume before 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 CA SAPCO before implementation. A CUA must be established before occupancy.

b. Before creating a SAPCA in a SCIF or using sensitive compartmented information (SCI) in a SAPF or SAPCA, a CUA will be established in accordance with Enclosure 2 of Volume 2 of DoD Manual (DoDM) 5105.21 (Reference (i)).

8. PHYSICAL ACCESS CONTROLS

a. Each SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA will have procedures for identification and control of visitors seeking physical access in accordance with this volume and Reference (f). Personal introduction and identification should be used to the maximum extent.

b. When all individuals within a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA cannot be personally identified, a badging system may be required by the PSO. This normally occurs when a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA hosts more than 25 people.

(1) When a badge system is considered necessary, it will be documented in the standard operating procedures (SOPs) and address topics such as badge accountability, storage, disposition, destruction, format, and use.

(2) If card readers are used in conjunction with badges and a means exists to lock out lost, unused, and relinquished badges, the PSO or GSSO may negate the requirements in this section for badge inventory, accountability, and destruction.

c. When not occupied, SAPFs and T-SAPFs will be alarmed in secure mode and secured with an approved General Services Administration (GSA) FF-L2740A combination lock in accordance with Federal Specification FF-L 2740B (Reference (j)).

d. Access control to a SAPCA will be accomplished by mechanical or electronic access control devices only. Spin-dial combination locks (e.g., XO series locks) will not be installed on SAPCA doors and independent alarm systems will not be installed in a SAPCA. Intrusion sensors will be installed when the SAPCA includes an exterior boundary wall of the parent SAPF or SCIF.

9. CONTROL OF COMBINATIONS

a. Combinations to locks will not be the same throughout a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA (e.g., doors, vaults).

b. Combinations to locks installed on security containers, safes, perimeter doors, windows, and any other opening will be changed when:

(1) A combination lock is first installed or used.

(2) A combination has been subjected, or believed to have been subjected, to compromise.

(3) A person knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock.

(4) The PSO, GSSO, or CPSO considers the change necessary.

c. When the lock is taken out of service, the combination will be reset to 50-25-50. Unserviceable high-security padlocks, keys, and cylinders will be controlled until properly destroyed. These high-security padlocks, cylinders, and keys can be sent to the DoD Lock Program for disposal at the following addresses:

(1) For Navy, Marine Corps, and Coast Guard, ship via registered mail to:

Commanding Officer
Naval Surface Warfare Center,
Crane, IN 47522-5010
(Code GXQS)

(2) For all other DoD Components, ship via registered mail to:

DoD Lock Program (HSPS)
1100 23rd Avenue
Port Hueneme, CA 93043-4370

d. All combinations to the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA entrance doors should be stored in a different SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA accredited at the same or higher classification level and handling caveat. When this is not feasible, the PSO or GSSO will prescribe alternative storage locations.

e. Safe combinations will be safeguarded at the highest level of classification and handling caveats of the material stored.

10. ENTRY-EXIT INSPECTIONS. The SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA will have procedures for inspecting personal belongings and vehicles at the entry and exit points, or at other designated areas, and points of entry to the building or site. Inspections will deter the unauthorized removal of classified material and the introduction of prohibited items or contraband. Legal counsel should review all personnel inspection procedures before distribution.

11. CONTROL OF ELECTRONIC DEVICES AND OTHER ITEMS

a. The SOP will contain guidance for control of portable electronic devices (PEDs) and other items introduced into or removed from the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA.

b. The following PEDs without loadable data storage capabilities are authorized within the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA. Medical devices with a two-way capability require approval by the PSO or SAO.

(1) Electronic calculators, spell checkers, language translators, etc.

(2) Receive-only pagers.

(3) Audio and video playback devices.

(4) Receive-only radios.

(5) Devices that do not transfer, receive, store, or generate data (text, audio, video, etc.).

c. Designated areas may be identified at the entry point to all SAP areas for the storage of PEDs. Where PED storage areas or containers are allowed by the PSO to be within the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA, the PEDs will be turned off. These designated PED storage areas or containers will be confined to designated "non-discussion" areas.

d. Mission-essential government- or contractor- owned PEDs introduced into the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA will be approved by the PSO and AO or designee in accordance with Reference (f) before entering the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA.

e. The prohibition of PEDs in SAPFs, T-SAPFs, SAPCAs, SAPWAs, and SAPTSWAs does not apply to those needed by persons with disabilities or for medical or health reasons (e.g., motorized wheelchairs, hearing aids, heart pacemakers, amplified telephone headsets, teletypewriters for the hearing impaired). The PSO, GSSO, or CPSO will establish procedures within the SOP for notification that such equipment is being brought into the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA.

f. Emergency personnel or first responders and their equipment, including devices carried by emergency medical personnel, responding to a medical crisis within a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA, will be admitted without regard to their security clearance status. Emergency personnel will be escorted to the degree practical. As appropriate, arrangements will be made for the debriefing of emergency personnel as soon as possible.

g. Waivers to this policy must be in writing and approved by the Director, CA SAPCO or designee. Requests for waivers must be submitted by the SAO and:

(1) Approved on a case-by-case basis based on mission requirements.

(2) Coordinated with the appropriate authorizing official for each affected information system within the SAP accredited area.

(3) Identify mitigations.

(4) Identify risks (after mitigation) to classified information.

h. If the CA SAPCO approves the waiver, the facility SOP will be revised to define the procedures and guidance for control of PEDs and other items introduced into or removed from the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA. In addition, any tenant SAP PSOs will

be notified in writing and informed the facility is accredited with waiver for appropriate action by the tenant CA SAPCO.

12. TEMPEST REQUIREMENTS

a. When compliance with TEMPEST standards is required, the PSO or SAO will issue specific guidance in accordance with current national directives that afford consideration to realistic, validated local threats as well as cost effectiveness.

b. A CTTA must conduct or validate all TEMPEST countermeasure reviews in accordance with Reference (f) and the Committee on National Security Instruction 7000 (Reference (k)).

c. If a TEMPEST countermeasure review has been completed, and the CTTA has determined that TEMPEST countermeasures are required, the CTTA will recommend the most cost-effective countermeasure that will contain compromising emanations within the inspectable space.

d. Only those TEMPEST countermeasures recommended by CTTA and authorized by the government program manager or government contracting official should be implemented. The processing of classified national security information as defined in in Volume 3 of DoDM 5200.01 (Reference (l)) or the submission of information for a TEMPEST countermeasure review does not imply a requirement to implement TEMPEST countermeasures. TEMPEST countermeasures that CTTA may be recommend include, but are not limited to:

(1) The use of shielded enclosures or architectural shielding.

(2) The use of equipment that has TEMPEST profiles or TEMPEST zones that match the inspectable space, distance, or zone respectively.

(3) The use of RED and BLACK separation installation guidance in accordance with Committee on National Security Systems Advisory Memorandum TEMPEST/01-13 (Reference (m)).

e. Telephone line filters, power filters, and non-conductive disconnects are not required for TEMPEST purposes, unless recommended by a CTTA as part of a TEMPEST countermeasure requirement. Telephone line disconnects, not to be confused with telephone line filters, may be required for non-TEMPEST purposes.

13. TWO PERSON INTEGRITY (TPI). TPI mandates the minimum of two indoctrinated persons at all times in a SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA. This security protection can only be authorized by the Director, CA SAPCO or designee, and reflected in the SOP.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CA	cognizant authority
CSP	construction security plan
CPSO	contractor program security officer
CTTA	certified TEMPEST technical authority
CUA	co-utilization agreement
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DSS	Defense Security Service
FCL	facility security clearance
FFC	fixed facility checklist
GSA	General Services Administration
GSSO	government SAP security officer
OA	oversight authority
PED	portable electronic device
PSA	principal staff assistant
PSO	program security officer
SAO	special access program facility accrediting official
SAP	special access program
SAPCA	special access program compartmented area
SAPCO	Special Access Program Central Office
SAPF	special access program facility
SAPTSWA	special access program temporary secure working area
SAPWA	special access program working area
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SID	security in depth
SOP	standard operating procedures
TPI	two person integrity
T-SAPF	temporary special access program facility
TSCM	technical surveillance countermeasures
USD(I&S)	Under Secretary of Defense for Intelligence and Security

PART II. DEFINITIONS

Unless otherwise indicated, these terms and their definitions are for the purposes of this volume.

accreditation. The formal approval of a specific place, referred to as a SAPF, that meets prescribed physical, technical, and personnel security standards.

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

continuous operation. This condition exists when a SAPF is staffed 24 hours every day.

co-utilization. Two or more organizations that share the same SAPF.

CTTA. Defined in Reference (k).

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

RED and BLACK separation. The segregation of equipment that processes classified information (RED) from equipment that processes unclassified information (BLACK) in unique, isolated areas. This partition prevents the inadvertent transmission of classified data over telephone lines, power lines, signal lines, and electrical components, circuits, and communication media.

SAO. A properly trained SAP facility accrediting official designated by the CA SAPCO to physically inspect and review and approve or disapprove physical security preconstruction plans for a SAPF, T-SAPF, SAPCA, and SAPWA or SAPTSWA before accreditation.

SAPCA. A room or set of rooms located within a SAPF or SCIF that is designed to enforce need-to-know. A SAPCA is required when different compartmented programs are sharing the same SAPF or SCIF and when not all personnel are cross-briefed.

SAPF. An accredited area, room, group of rooms, building, or installation where SAP materials may be stored, used, discussed, manufactured, or electronically processed. SAPFs include, but are not limited to, fixed facilities, mobile platforms, prefabricated structures, containers, modular applications, or other new or emerging applications and technologies that may meet performance standards for use in SAPF construction.

SAPTSWA. An accredited area normally used for meetings involving the discussion or processing of SAP information, when use is limited to less than 40 hours per month.

SAPWA. An accredited area used for discussing, handling, or processing SAP, but where storage is not authorized.

SCI. 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 National Intelligence.

SCIF. An accredited area, room, group of rooms, building, or installation where SCI may be stored, used, discussed, or electronically processed.

SID. A determination made by the SAO that a facility's security SAP consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. SID describes the factors that enhance the probability of detection before actual penetration to the SAPF. The existence of a layer or layers of security that offer mitigations for risks may be accepted by the SAO.

site security manager. Defined in Reference (g).

TEMPEST. The investigation and study of compromising emanations.

T-SAPF. SAPF designed to be temporary or such as those at sites for contingency operations, emergency operations, and tactical military operations meeting the requirements of chapter 6 of Reference (f).

TSCM. Techniques and measures to detect, neutralize, and exploit a wide variety of hostile and foreign penetration technologies that are used to obtain unauthorized access to classified and sensitive information.

TSCM evaluations. A physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration.

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

waiver. An exemption to the security requirements of this volume.