# Department of Defense
# MANUAL

**NUMBER** 5205.07, Volume 1
June 18, 2015

USD(I)

SUBJECT: DoD Special Access Program (SAP) Security Manual: General Procedures

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) Assigns responsibilities, implements policy established in DoD Instruction (DoDI) 5205.11 (Reference (c)), and describes the general procedures for the administration of DoD SAP security.

(2) Incorporates and cancels Revision 1 Department of Defense Overprint to the National Industrial Security Program (NISP) Operating Manual Supplement (Reference (d)).

2. APPLICABILITY. This volume applies to:

a. 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").

b. All DoD Component contractors and consultants who require access to DoD SAPs pursuant to the terms and conditions of the contract or agreement.

c. Non-DoD U.S. Government (USG) 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 (MOA) or other interagency agreement established with the DoD.

3. POLICY. It is DoD policy according to 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. Follow the procedures in Reference (b), those in Enclosures 3-12 of this volume, and the processing procedures and templates posted on the Defense Security Service (DSS) Website found at http://www.dss.mil/isp/specialprograms.html. Requests for clarification of this volume will be forwarded through the Program Security Officer to the cognizant authority (CA) SAP Central Office (SAPCO) for resolution. The SAPCO can contact the Office of the Under Secretary of Defense for Intelligence (USD(I)) for SAP security policy clarification as needed.

6. RELEASABILITY. **Cleared for public release**. This volume is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This volume is effective June 18, 2015.

Marcel Lettre
Acting Under Secretary of Defense
for Intelligence

Enclosures

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))," October 24, 2014, as amended
(b) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010
(c) DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)", February 6, 2013
(d) Revision 1 Department of Defense Overprint to the National Industrial Security Program Operating Manual Supplement, April 1, 2004 (hereby cancelled)
(e) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011
(f) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985
(g) DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended
(h) DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, as amended
(i) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(j) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015
(k) DoD Joint Special Access Program Implementation Guide (JSIG), October 9, 2013
(l) 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
(m) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012
(n) DoD Directive 2060.1, "Implementation of, and Compliance with, Arms Control Agreements," January 9, 2001
(o) DoD Directive 5240.02, "Counterintelligence," March 17, 2015
(p) DoD Instruction 5240.10, "Counterintelligence (CI) in the Combatant Commands and Other DoD Components," October 5, 2011, as amended
(q) National Policy and Procedures for the Disclosure of Classified Military Intelligence to Foreign Governments and International Organizations, short title: National Disclosure Policy-1 (NDP-1), October 1, 1988[1]
(r) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(s) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
(t) Executive Order 13526, "Classified National Security Information," December 29, 2009
(u) DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended
(v) Section 119 of Title 10, United States Code
(w) Part 2, Appendix D of Title 42, United States Code
(x) Committee on National Security Systems Policy (CNSSP) No. 22, "National Policy on Information Assurance Risk Management for National Security Systems," January, 2012

[1] Provided to designated disclosure authorities on a need-to-know basis from the Defense Technology Security Administration's International Security Directorate.

(y) Intelligence Community Directive Number 503, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation," September 15, 2008
(z) Directive-type Memorandum 09-012, "Interim Policy Guidance for DoD Physical Access Control," December 8, 2009, as amended
(aa) DoD Manual 5220.22, Volume 3, "National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)," April 17, 2014
(ab) Part 2004 of Title 32, Code of Federal Regulations

ENCLOSURE 2

RESPONSIBILITIES

1. USD(I). The Office of the USD(I) is the office of primary responsibility for the development and maintenance of this volume.

2. DIRECTOR, DSS. Under the authority, direction, and control of the USD(I), the Director, DSS:

a. Administers the NISP in accordance with DoDI 5220.22 (Reference (e)), DoD 5220.22-R (Reference (f)), and DoD 5220.22-M (Reference (g)).

b. Issues facility security clearances (FCLs) for defense contractors performing on all DoD classified contracts, to include contractors performing on DoD SAPs.

c. Unless a carve-out provision is approved by the Secretary of Defense or the Deputy Secretary of Defense:

(1) Performs SAP security inspections at cleared defense contractor locations in accordance with this volume, Reference (f), and the government contracting activity's completed DD Form 254, "Department of Defense Contract Security Classification Specification," located at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

(2) Authorizes classified contractor SAP information systems (ISs) and the introduction of guest systems in contractor SAP facilities (SAPFs).

(3) Coordinates with the designated counterintelligence (CI) component to provide cross-sharing of threat and incident information affecting the security of the facility or its defense information or cleared personnel.

d. Maintains and trains a cadre of personnel proficient in policies, procedures, and security, as codified in this manual.

3. DIRECTOR, DoD SAPCO. Under the authority, direction, and control of the Deputy Secretary of Defense, the Director, DoD SAPCO:

a. Serves as the DoD designated proponent for developing and implementing policies and procedures for DoD SAP execution, management, and administration.

b. Functions as the DoD single point of Congressional liaison concerning SAPs.

c. Supports departmental efforts to resolve issues and decisions related to SAP security, technology transfer, technology export, the Committee on Foreign Investment in the United

States, mutual participation by foreign partners, bilateral collaboration, and foreign ownership, control, and influence (FOCI).

4. DoD CIO. In coordination with the Director, DoD SAPCO, the DoD CIO:

a. Establishes and administers governance and risk management policies to develop enterprise SAP information technology (IT) strategy, telecommunications infrastructure policy, SAP network IT requirements, and network and systems funding oversight policy in accordance with Reference (c).

b. Develops and issues supplemental policies and procedures for cybersecurity and authorization of DoD SAP ISs.

c. Establishes requirements and participation parameters for secure networks, databases, and ISs that support SAP governance and reciprocity within the DoD SAP communities.

5. DoD COMPONENT HEADS AND OSD PRINCIPAL STAFF ASSISTANTS (PSAs) WITH CA AND OVERSIGHT AUTHORITY (OA) OVER SAPS. The DoD Component heads and the OSD PSAs with CA and OA over SAPs:

a. Identify an inspection official responsible for implementing a SAP compliance inspection program in accordance with Enclosure 9 of this volume.

b. Comply with DoD 8570.01-M (Reference (h)) for IA training requirements.

c. Coordinate with the DSS CI Directorate to provide cross-sharing of threat and incident information affecting the security of the facility or its defense information or cleared personnel and cleared contractors under the NISP when the SAP is carved out of DSS oversight.

6. DIRECTORS OF THE DoD COMPONENT SAPCOs AND DIRECTORS OF THE PSAs SAPCOs WITH CA AND OA OVER SAPs. Under the authority, direction, and control of their respective DoD Component heads and PSAs, the Directors of the DoD Component SAPCOs and the PSA SAPCOs with CA and OA over SAPs:

a. Develop policies and procedures for the implementation of the requirements of this volume within their respective component, as required.

b. Oversee, establish, and manage continuing security awareness training and program requirements to ensure complete, common, and continuing application of SAP security.

c. Establish a SAP Information Security program, defining SAP accountability requirements.

d. Provide support and oversight of their SAP IS security program.

e. Plan and budget for cybersecurity resources for SAPs under their purview.

# ENCLOSURE 3

# FUNCTIONAL ROLES

1. GOVERNMENT PROGRAM MANAGER (GPM). The GPM:

a. Manages designated SAPs.

b. Implements and executes SAP security countermeasures in accordance with all applicable laws; national, DoD, and DoD Component issuances relating to or governing DoD SAPs; and this volume.

c. Monitors and assigns personnel, financial resources, and facilities required to establish, support, and maintain SAPs and security compliance.

d. Implements operations security (OPSEC), treaty, and arms control measures needed to support the SAP and ensure a tailored Security Education and Training Awareness (SETA) program for all briefed personnel.

e. Plans and budgets for program cybersecurity resources, ensuring compliance with established cybersecurity policy for all systems, including those under contract or vendor-provided.

f. Complies with applicable cybersecurity and technology acquisition requirements in accordance with DoDD 5000.01 (Reference (i)) and Interim DoDI 5000.02 (Reference (j)) for all IS acquisitions.

g. Serves as the IS Owner in accordance with the DoD Joint Special Access Program Implementation Guide (Reference (k)).

2. PSO. The PSO, appointed by the CA SAPCO, is responsible for the program security management and execution of all security policies and requirements for a specific SAP(s) program(s), compartment(s), sub-compartment(s), or project(s), and:

a. Works with the GPM to develop, implement, and enforce a security program that protects all facets of the SAP. Provides security subject matter expertise to the GPM and oversight to assigned programs to ensure compliance with all established policy and procedures.

b. Provides oversight and direction for SETA programs.

c. Provides oversight and direction to government SAP security officers (GSSOs) and contractor program security officers (CPSOs) designated to support SAPs.

d. Conducts or verifies that all approved SAPFs are properly inspected for security compliance.

e. In coordination with the appropriate government CI activity, applies risk management principles to SAP security architectures and environments for which the PSO is responsible. These principles include but are not limited to:

(1) Identify, characterize, and assess threats.

(2) Assess the vulnerability of critical assets to specific threats.

(3) Determine the risk (i.e., the expected likelihood and consequences of specific types of attacks on specific assets).

(4) Identify ways to mitigate those risks.

(5) Identify and assess cost and resources to mitigate those risks.

(6) Prioritize risk mitigation measures based on a strategy.

f. Approves changes to the environment and operational needs that could affect the security authorization in accordance with Reference (k).

g. Verifies that configuration management policies and procedures for authorizing the use of hardware and software on an IS are followed in accordance with Reference (k).

h. Ensures that each assigned GSSO and CPSO conducts and documents annual self-inspection. Approves the resultant corrective actions to establish or ensure compliance.

i. Ensures that a SAP trained and knowledgeable GSSO or CPSO, as appropriate, is assigned to serve as the SAP security official at each organization or facility.

j. Initiates and directs security investigations and inquiries to fully explore and document security incidents.

3. GSSOs and CPSOs. GSSOs and CPSOs:

a. Coordinate with the PSO and the GPM or Contractor Program Manager (CPM), respectively, to create a secure environment to facilitate the successful development and execution of a SAP(s) at each organization or location where SAP information is stored, accessed, or SAP-accessed personnel are assigned.

b. Are responsible for security management, to include SETA, and operations within their assigned activity, organization, or office.

c. Adhere to applicable laws as well as national, DoD, and other security SAP policies and requirements.

d. Coordinate SAP security matters with the PSO and GPM or CPM, respectively.

e. Establish, conduct, and document initial, event-driven, and annual refresher training for all assigned SAP-accessed individuals.

f. Conduct an annual self-inspection, document the self-inspection, and submit to the PSO a corrective action plan that identifies actions to establish compliance.

4. CPM. CPMs will:

a. Assign in writing a CPSO to serve as the SAP security official at each contractor organization or location where SAP information is stored or accessed or SAP-accessed personnel are assigned.

b. Be responsible for execution for the statement of work, contract, task orders, and all other contractual obligations.

5. TOP SECRET (TS) CONTROL OFFICER (TSCO). TSCOs will be responsible for the receipt, dispatch, transmission, and maintenance of access, accountability, and inventory records for TS SAP material. TSCOs will be designated in writing by the GPM or CPM, when the PSO determines a program requires a TSCO. The processes used by the TSCO will be thoroughly documented in the standard operating procedures (SOPs).

# ENCLOSURE 4

# GENERAL PROVISIONS AND REQUIREMENTS

1. SOP.

a. The GSSO or CPSO will prepare SOPs to implement the security policies and requirements unique to their facilities and the SAP.

b. The GSSO or CPSO will forward the proposed SOPs and SOP changes to the PSO, for approval.

c. A SOP is not required for a pre-solicitation activity, a research and development announcement, a request for information, or a request for proposal when there is no contractual relationship established for that effort or when contractors perform SAP work at government facilities only and not at contractor facilities. In these instances, classification guidance and special security rules reflected on the DD Form 254 and in the Security Classification Guide (SCG) suffice as the SOP.

d. Special security instructions will be instituted outlining the procedures that protect the information and are compliant with the security policy reflected on the DD Form 254 and expressly incorporated into the contract.

e. A SOP template is posted on the DSS website at http://www.dss.mil/isp/specialprograms.html. At a minimum, the following topics will be addressed in the SOP:

(1) General provision and requirements.

(2) Reporting requirements.

(3) Security clearances.

(4) SETA program.

(5) Classification and markings.

(6) Safeguarding classified information.

(7) Visits and meetings.

(8) Subcontracting.

(9) ISs.

2. REPORTING REQUIREMENTS. Reports required based on this volume are posted on the DSS website at http://www.dss.mil/isp/specialprograms.html. At a minimum, report the following to the PSO:

a. Adverse Information

b. Refusal to sign a SAP Indoctrination Agreement

c. Change in Employee Status

d. Employees Desiring Not to Perform on SAP Classified Work

e. Foreign Travel

f. Changes or modifications to the SAP area accreditation

3. FRAUD, WASTE, ABUSE, AND CORRUPTION (FWAC).

a. Government and industry FWAC SAP reporting involving SAP information will be accomplished through SAP channels. Collateral FWAC reporting channels must not be used for SAP information.

b. The PSO will provide the telephone number for the current FWAC hotline for reporting SAP information. FWAC reporting information will be conspicuously posted in the SAP workspace.

c. Employees do not need management approval before making reports.

4. CO-UTILIZATION AGREEMENT (CUA). The CUA documents areas of authorities and responsibilities between cognizant security offices (CSOs) when they share the same SAPF. A CUA will be executed between CSOs. The first CSO in an area, unless otherwise agreed upon, will be considered the host CSO responsible for all security oversight. The CUA will be initiated by the tenant PSO and approved by all parties before introduction of the additional SAP(s) into the SAPF.

a. Topics to be included in a CUA include: compliance inspection responsibility, incident notification, and host-tenant agreement to clarify inspection responsibilities. All CUAs will be reviewed and updated on a biannual basis.

b. Agencies desiring to co-utilize a SAPF will accept the current accreditation of the cognizant agency. Prospective tenant activities will be informed of all waivers to the requirements of this manual 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 appropriate CA SAPCO before implementation. Any changes to the approved CUA must be submitted to the appropriate PSOs before implementing the changes.

c. For CUAs, the responsible organization will be identified for executing security cognizance with a carved-out SAP.

d. Co-utilization of Sensitive Compartmented Information (SCI) within a SAPF, or SAP within an SCI facility, will require authorization from the PSO and the servicing special security officer in accordance with Volume 2 of DoD Manual (DoDM) 5105.21 (Reference (l)).

5. OPSEC. All SAPs will have an OPSEC program developed and maintained in accordance with DoDD 5205.02E (Reference (m)).

6. PROGRAM PROTECTION PLAN (PPP). All SAPs will develop, implement, and maintain a PPP or alternative documents that, when combined, meet the intent of the PPP.

7. PATENTS AND INTELLECTUAL PROPERTY. The CA SAPCO will develop procedures for processing patents and intellectual property involving SAP(s).

8. ARMS CONTROL AND TREATIES.

a. DoDD 2060.1 (Reference (n)) establishes the arms control implementation and compliance responsibilities for SAPs; in accordance with Reference (b), treaty compliance requirements, obligations, or constraints will be considered as an integral part of the policy. DoD SAPs must be prepared to comply with treaties and agreements to which the USG is a signatory. DoD SAPs will be protected against unnecessary or inadvertent exposure during USG participation in authorized verification activities, confidence-building measures, and over flights.

b. The PSO, GSSO, and CPSO should be familiar with various arms control verification activities in order to exercise security oversight for SAPs. Arms control treaty guidance and procedures are located at the website http://www.dss.mil/isp/specialprograms.html.

9. LITIGATION AND PUBLIC PROCEEDINGS.

a. Threatened or actual litigation, administrative investigations or inquiries, or public proceedings at the international, federal, State, tribal, or local levels that may involve a SAP will be reported to CA SAPCO. Appropriate DoD general counsel offices or judge advocate offices will be notified of potential litigation issues at the earliest possible time. These proceedings include legal or administrative actions in which the prime contractor, subcontractors, or government organizations and SAP-accessed individuals are a named party (plaintiff, defendant, or witness).

b. DoD government and contractor personnel accessed to DoD SAPs will inform the PSO of any litigation actions that may pertain to the SAP, to include litigation regarding the physical environments, facilities, or personnel, or as otherwise directed by the GPM. PSOs will be notified of employee or union strikes, employer discrimination complaints, Equal Employment Opportunity cases, Merit Service Protection Board appeals, litigation, etc. in accordance with the timelines required by Enclosure 2, paragraph 5.s of Reference (c).

10. CI SUPPORT.

a. Analysis of foreign intelligence threats and risks to SAP information, material, personnel, and activities will be undertaken in accordance with DoDD O-5240.02 (Reference (o)); by the organic CI organization or by the lead military department CI organization in accordance with DoDI 5240.10 (Reference (p)). Information that may have a bearing on the security of a SAP will be provided by the government or military CI agency to the affected SAP PM and PSO, as necessary.

b. Contractors may use CI support to enhance or assist security planning and safeguarding in pursuit of satisfying contractual obligations. Requests for SAP-applicable CI support will be made to the respective PSO before contractors receiving such support.

11. COMMUNICATIONS SECURITY. SAP information will be electronically transmitted by approved secure communications channels authorized by the SOP.

12. INTERNATIONAL SAP SECURITY REQUIREMENTS.

a. The National Disclosure Policy (NDP-1) (Reference (q)) governs all foreign disclosures of classified military information. Security planning for foreign disclosure is an ongoing process that requires reviews at each milestone in the SAP lifecycle.

(1) All SAPs will comply with Reference (q). SAPs will include foreign disclosure and security planning at the beginning of the prospective SAP process or at the earliest possible date foreign disclosure is identified in an ongoing SAP. When a SAP is identified for international cooperation or foreign disclosure, all foreign disclosure and policy guidance will be in accordance with Reference (q), DoDD 5230.11 (Reference (r)), and DoDD 5530.3 (Reference (s)).

(2) The foreign disclosure officer and CA SAPCO do not have authority to disclose SAPs without Secretary of Defense or Deputy Secretary of Defense approval, in accordance with Reference (b).

b. The GPM and PSO will coordinate with their Component Foreign Disclosure Office and CA SAPCO to develop technology assessment or control plans, MOAs, and security

documentation for all international SAPs as appropriate. Additional security requirements are further identified in bilateral program-specific security agreements, General Security of Military Information Agreements, and Industrial Security Arrangements.

ENCLOSURE 5

SAFEGUARDING CLASSIFIED INFORMATION

1. HANDLE VIA SPECIAL ACCESS CHANNELS ONLY (HVSACO).

a. The purposes of HVSACO are:

(1) To preclude the disclosure of general program-related information outside established acknowledged and unacknowledged SAP channels.

(2) To minimize OPSEC indicators.

(3) To facilitate communication of information within SAPs.

b. Dissemination of information warranting HVSACO protection will be limited to persons briefed into a SAP and retained within SAP approved channels. Formal SAP indoctrination or execution of briefing or debriefing forms specifically for HVSACO is not required. The term SAP channels denote secure, approved SAP communications systems, SAPFs, or PSO-approved SAP storage areas. HVSACO is not a classification level, but rather a protection or handling system. Examples of HVSACO uses may include:

(1) For general non-program specific communications between and within SAPs. More specifically, on information related to SAP security procedures, test plans, transportation plans, manufacturing plans, and notional concepts related to research, development, testing, and evaluation of SAPs.

(2) When a paragraph or document contains information that is unique to a SAP and its distribution.

(3) When necessary to protect sensitive relationships.

(4) To protect information that does not warrant classification under Executive Order 13526 (Reference (t)).

(5) When using a SAP nickname for an unacknowledged SAP.

c. Upon request for public release, the originator of the material must review the material involved to determine whether to retain it within program channels:

(1) If public release is appropriate, remove the HVSACO marking from the document; or

(2) Inform the requestor of the decision not to release the information, citing an appropriate authority.

d. Training on HVSACO should be included in annual security awareness refresher sessions.

e. Procedures for the use of HVSACO should be included in Program SCGs.

f. Materials warranting HVSACO protection must be stored in accordance with the SOP. Unclassified HVSACO materials may be stored openly within an approved SAPF taking into account OPSEC considerations. PSOs may grant an exception to allow the taking of unclassified HVSACO materials to alternate temporary storage areas, provided the material is under an appropriately authorized individual's direct control, or under "key lock protection" which is controlled by that individual.

g. Transmission of SAP material.

(1) At a minimum, use U.S. First Class mail for shipment of unclassified materials requiring HVSACO protection.

(2) Use the secure mode when discussing HVSACO-protected material on authorized telephones.

(3) Use only approved, secure facsimile (FAX) equipment when transmitting HVSACO-protected material.

(4) Do not transmit HVSACO-protected material via unclassified e-mail.

h. Reproduce unclassified HVSACO-protected information only on equipment approved by the PSO.

i. HVSACO protection does not require accountability. Document accountability is based on classification level or unique program requirements. Document control numbers, entry into document control systems, or internal or external receipts are not required for unclassified HVSACO-protected material.

j. Destroy HVSACO-protected information according to the procedures approved for classified material. Destruction certificates are not required for non-accountable HVSACO-protected materials.

k. Based on an assessment of the OPSEC risk, notify the PSO within 24 hours of any possible improper handling or misuse of HVSACO-protected information and its impact. An inquiry should be conducted to determine if a compromise occurred as a result of practices dangerous to security. The PSO will ensure that prompt corrective action is taken on any practices dangerous to security.

l. Contact the originating office for permission to remove HVSACO markings.

2. USE OF SECURE ENCRYPTION DEVICES AND ELECTRONIC TRANSMISSION EQUIPMENT.

a. Secure Encryption Devices.

(1) SAP government and industry organizations must use National Security Agency/Central Security Service (NSA/CSS) approved or certified Type I encrypted secure communications for the electronic transmission of all classified information.

(2) All products used for the electrical transmission of classified or sensitive information must be used in accordance with prescribed national and associated policies or doctrine.

b. Secure FAX. Secure FAX encrypted communications equipment may be used for the transmission of SAP information. When secure FAX is permitted, the PSO will approve the system in writing.

(1) Do not use FAX terminals equipped with the automatic polling function enabled unless authorized by the PSO.

(2) When approved by the PSO, SAP documents classified SECRET (S) SAP and below may be receipted via an automated generated message that confirms undisturbed transmission and receipt. A transmission log will be maintained and validated during GSSO or CPSO self-inspections and made available for review during inspections.

(3) When transmitting TS SAP documents over a secure FAX terminal, the recipient must acknowledge receipt of the TS SAP material. The recipient will return a signed receipt after completion of transmission. The transmission and receipt of TS material will be recorded by the sender in a FAX log.

c. Electronic Transmission. When using electronic transmission (e.g., voice over internet protocol, video teleconferencing for SAP material), encrypted communications equipment will be used. When secure electronic transmission is permitted, the authorizing official, in coordination with the PSO, will approve the system in writing to the GSSO or CPSO.

3. CONTROL. SAP classified material, hardware, equipment and all media not subject to accountability will be controlled by the procedures implemented by policy, training, and awareness that:

a. Regulate and monitor the introduction and exit of all controlled items from all SAPFs.

b. Identify and document:

(1) The identity of the custodian, date created (or entered the SAPFs) and date destroyed (or exited the SAPFs).

(2) Classification, Program sensitivity (e.g. TS, S//SAR-XYZ, U//HVSACO, For Official Use Only (FOUO), Unclassified (U), personally identifiable information).

(3) Type (e.g. documents, hard disks, compact disks, universal serial bus storage devices).

(4) Content (e.g., application software, non-writable or writable, engineering notebook).

c. At least on an annual basis, the continued need for all controlled items will be assessed and items no longer required will be destroyed.

d. Safeguarding of classified information, to include SAP material, will be done in accordance with Volume 3 of DoDM 5200.01 (Reference (u)), unless otherwise noted in this volume.

4. ACCOUNTABILITY.

a. An accountability system approved by the PSO will be developed and maintained for the following SAP classified information.

(1) All TS SAP material, media, hardware, equipment, etc.

(2) S SAP material, media, hardware, equipment, etc. when directed by the CA SAPCO.

(3) All other classified media when directed by the CA SAPCO.

b. Accountable SAP material will be entered into an accountability system whenever it is received, generated, reproduced, or dispatched either internally or externally to other SAPFs. The accountability system will be designed to record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction. The accountability system will assign individual responsibility for all accountable information. An automated system, if used, will have a backup. When SAP material is received with the originator's accountability control number, the accountability system will include the originator's accountability control number.

c. The accountability system will have at the minimum:

(1) Classification.

(2) Originator of the item.

(3) Title and description of item.

(4) Custodian assigned.

(5) Date of product.

(6) Control number (maintained in consecutive number series).

(7) Copy number.

(8) Page count.

(9) Disposition and date.

(10) Destruction date.

(11) Internal and external receipt records

d. A disclosure sheet will be maintained for each TS item. The name is recorded only once regardless of the number of times subsequent access occurs. Once destruction of a TS product takes place, the TS access record will be kept with the destruction paperwork and destroyed 3 years after the document is destroyed.

e. Electronic files do not need to be placed into accountability systems or the information management system referenced in paragraph 4a of this enclosure when residing on ISs or receipted when transmitted between system users within the same unified network provided the data remains resident within the IS.

## 5. ANNUAL INVENTORY.

a. A 100 percent inventory of accountable SAP material will be conducted annually by the individual responsible for the control system or their alternate and a disinterested party. The annual inventory date will not exceed the previous year's inventory date by more than 12 months. Inventories will be conducted by visual inspection of all items of accountable SAP material and verification of pertinent information (originator, date, subject, file number, etc.) and page count for TS SAP held within the SAPF.

b. Inventories of TS material will be documented by the TSCO and a second disinterested individual and made available during security compliance inspections. Discrepancies will be reported immediately to the PSO, who will ensure action is taken, as appropriate, in accordance with Enclosure 8 of this volume.

## 6. COLLATERAL CLASSIFIED MATERIAL.

a. The PSO will provide oversight for collateral classified material maintained in the SAP. The process for introduction of collateral material will be approved by the PSO. Collateral material assigned or produced under a collateral contract required to support a SAP will be PSO-approved before the introduction, inclusion, or production, and may be transferred within SAP controls.

b. Transfer will be accomplished in a manner that will not compromise the SAP or any classified information. Collateral classified material generated during the performance of a SAP contract may be transferred from the SAP to another SAP or collateral program.

7. TRANSMISSION AND PREPARATION OF SAP CLASSIFIED MATERIAL.

a. SAP information will only be transmitted outside the SAPF using one of the methods identified within this section. The GSSO or CPSO will oversee transmission of SAP material. The order of precedence for transmission processes is:

(1) Cryptographic communications systems (i.e., secure facsimile, IS).

(2) Courier.

(3) PSO approved government or commercial carrier for S SAP material and below.

(4) Defense Courier Service for TS SAP material.

(5) United States Postal Service (USPS) registered mail or US Express Mail for S SAP material and below within the continental United States (CONUS).

(6) USPS certified mail for CONFIDENTIAL SAP material and below within CONUS.

b. SAP material being mailed or couriered will be prepared, reproduced, and packaged by the appropriately cleared SAP-briefed personnel inside the SAPF.

(1) Dispatch receipts are required for the transmission of SAP material.

(2) Classify receipts according to content.

(3) Inner and outer wrapping markings.

(a) Inner wrappings will be opaque and marked with the "TO" and "FROM" blocks and will bear the highest level of classification marking of the content.

(b) Outer wrappings will be opaque and will show an unclassified address on the "TO" and "FROM" blocks.

(4) When a receipt is not returned within 15 days, contact the recipient to determine status of the material. If the material is received, have the recipient provide the receipt. If the recipient did not receive the material, immediately initiate a preliminary inquiry and inform the PSO and the GPM.

c. SAP material will be transported from one SAPF to another in an unobtrusive and secure manner.

(1) Courier(s) must be accessed to the level of SAP being couriered.

(2) For local travel, SAP material may be hand-carried using a locked container as the outer wrapper. Local travel will be defined by CA SAPCO. Travel outside of the defined local area of the originating SAPF requires PSO approval. Attach a tag or label with the individual's name, organization, and telephone number.

(3) Travel should be performed using a personal, company owned, rented, or government vehicle. Use of public transportation requires PSO approval.

(4) TS SAP working papers taken to another SAPF in the same building for collaboration that will be returned before the expiration of the working paper time limits does not need to be placed into accountability when leaving the SAPF. Hand receipts documenting item and page count are still required.

d. When approved by the PSO, a USPS mailing channel may be established to ensure mail is received only by appropriately cleared and accessed personnel. Use USPS-registered mail or USPS Express Mail for S SAP material. Use USPS certified mail for CONFIDENTIAL SAP. "For Official Use Only" and unclassified HVSACO, material may be sent by First Class mail. When associations present an OPSEC concern in receiving and sending mail, the GSSO or CPSO will establish and use a sterile Post Office box with the written approval from the PSO.

(1) Except for TS SAP material, a USG-approved contract carrier (i.e., USPS Express Mail) can be used for overnight transmission on a case-by-case basis with approval of the PSO. Packages may only be shipped on Monday through Thursday and delivery date must be checked to ensure that the carrier does not retain the classified package over a holiday or weekend.

(2) These methods of transmitting selected SAP information are in addition to, not a replacement for, other transmission means previously approved for such material. Use of secure electronic means is the preferred method of transmission.

(3) Except for approved USPS means, use overnight delivery only when:

(a) Written approval is received by the PSO.

(b) SAP requirements dictate.

(c) Essential to mission accomplishment.

(d) Time is of the essence, negating other approved methods of transmission.

(e) Receiver of material will be readily available to sign upon arrival.

(4) To ensure direct delivery to address provided by the PSO:

(a) Do not execute the waiver of signature and indemnity on USPS label.

(b) Do not execute the release portion on commercial carrier forms.

(c) Ensure an appropriate recipient is designated and available to receive material.

(d) Do not disclose to the express service carrier that the package contains classified material.

(5) Immediately report any problem, misplaced, or non-delivery, loss, or other security incident encountered with this transmission means to the PSO.

e. The GSSO or CPSO will provide detailed courier instructions and training to SAP-briefed couriers when hand-carrying SAP information. Problems encountered will be immediately reported to the PSO, who may authorize exceptions when operational considerations or emergency situations dictate. The following rules will be adhered to when couriering classified material:

(1) The responsible PSO is required to approve all couriering of TS SAP material. Two-person courier teams are required for all TS SAP material unless a single courier is authorized in writing by the PSO. The courier must be accessed to the level of SAP information being couriered.

(2) A single-person courier may be used for S SAP and below materials.

(3) Provisions will be made for additional couriers and overnight storage, when required (regardless of classification), when it appears continuous vigilance over the material cannot be sustained by a single individual.

(4) As a minimum, the GSSO or CPSO from the departure location will provide each authorized courier with a copy of Department of Defense (DD) Form 2501, "Courier Authorization," based on instructions located at http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage1828.html or a PSO approved locally produced courier authorization memorandum.

(a) At a minimum, the courier authorization and instructions will address:

1. Method of transportation.

2. Travel itinerary (intermittent or unscheduled stops, remain-overnight scenario), specific courier responsibilities (primary or alternate roles, as necessary).

3. Completion of receipts, as necessary, and full identification of the classified data being transferred.

4. A discussion of emergency or contingency plans (include after-hours points of contact, primary or alternate contact data, telephone numbers).

5. Each courier will acknowledge receipt and understanding of this briefing in writing.

(b) Experienced SAP-briefed individuals who frequently or routinely perform duties as classified couriers may be issued courier authorization cards or DD Form 2501 by the GSSO or CPSO in lieu of individual letters for each trip. The form is issued for no more than 1 year at a time. The requirement for authorization to hand carry will be revalidated on at least an annual basis and a new form issued, if appropriate.

8. AIRPORT-SCREENING GUIDELINES FOR HANDLING CLASSIFIED MATERIAL.

a. Travel to and from locations in the U.S. aboard commercial or government carriers.

(1) PSOs will apprise couriers of the limitations and restrictions surrounding screening procedures. Notifying government screening officials of courier status is not required until screening officials request to inspect classified material.

(2) When screening officials request to inspect classified material, couriers will:

(a) Allow the classified material to undergo the x-ray examination.

(b) Divest any material that may trigger the automated screening equipment.

(c) Place all metal objects and electronics on the x-ray belt or in a second bag.

(d) If the screening official desires to inspect the package after x-ray screening, the courier will:

1. Present the courier authorization letter and their government-issued identification.

2. Request assistance from the screening official's supervisor.

3. Request a private screening.

4. Permit the supervisor to inspect the outer package but not the contents. If the screening supervisor cannot determine if the material is cleared for transport, the courier will contact the originating PSO for further instructions.

b. Travel to or from locations outside the United States. Classified information will be sent via secure classified networks, classified FAX, or diplomatic pouch whenever possible. Hand-

carrying SAP material other than by diplomatic courier should be used only as a last resort. Couriering classified SAP material on commercial aircraft is only approved by waiver issued by the Director, CA SAPCO, or designee.

c. Transportation Security Administration (TSA) Guidelines. The TSA publishes airport screening guidelines for handling classified material. GSSOs and CPSOs will ensure couriers are aware of the limitations and restrictions surrounding screening procedures.

9. TRANSPORTATION PLANS. The GSSO or CPSO will develop a transportation plan coordinated with and approved by the PSO at least 30 days in advance of the proposed movement. The transportation plan must:

a. Appoint a SAP-accessed individual knowledgeable about SAP security requirements to serve as the focal point for transportation issues.

b. Ensure that the planning includes priority of transportation modes (government surface, air, commercial surface, air) and inventory of classified SAP material to ensure SAP integrity.

c. Maintain a continuous chain of custody between the origination and destination, and comply with all Department of Transportation laws and SAP security requirements.

d. Include contingency planning (a description of emergency procedures, and who is responsible for actions that must be taken in the event of an emergency, e.g., unexpected stop anywhere along the route). Identify individuals by name, and provide their organization, telephone and fax numbers, and e-mail addresses.

e. Ensure CI support is incorporated into transportation planning and execution.

10. RELEASE OF INFORMATION.

a. Public release of SAP information is not authorized without written authority from the government in accordance with subtitle A, part 1, chapter 2, section 119 of Title 10 United States Code (U.S.C.) (Reference (v)) and part 2, appendix d of Title 42 U.S.C. (Reference (w)). Personnel are responsible to report any attempt by unauthorized personnel to obtain SAP information immediately to the PSO to the GPM.

(1) Information concerning SAPs must not be released to any non-SAP-accessed individual, firm, agency, or government activity without SAPCO approval. Classified or sensitive information concerning SAPs must not be included in general or unclassified publications, technical review documents, or marketing literature.

(2) All material proposed for release will be submitted through the PSO to the GPM 60 days before the proposed release date. After approval is granted, additional case-by-case requests to release identical data are not required.

b. Personnel currently or previously accessed to a SAP will provide the GPM and PSO with a copy of any proposed intended release of information that could potentially contain SAP information for review before public release. Information considered for release such as models, software, and technology that may impact other SAPs will require additional coordination with the DoD SAPCO, and other Component SAPCOs before release. The information and materials proposed for release will remain within SAP security channels until authorized for release.

c. The Defense Technical Information Center or the U.S. Department of Energy Office of Scientific and Technical Information does not accept SAP information.

d. Each SAP security officer will ensure the area SOP contains a process to ensure documents such as award nominations, performance reports, evaluations, etc. are reviewed to eliminate any program sensitive information before further dissemination.

11. REPRODUCTION.

a. SAP information will only be reproduced on equipment approved by the PSO. The GSSOs or CPSOs will prepare written reproduction procedures, and post a notice indicating if equipment can or cannot be used for reproduction of classified SAP material within a SAPF, and who is authorized to reproduce such material. Maintenance procedures will be written and incorporated into the SOPs listing the actions necessary when non-SAP briefed maintenance technicians' work on the equipment. When possible, an additional hard drive for maintenance purposes only should be purchased.

b. Equipment may be used outside a SAPF (e.g., within a SAP working area), provided written procedures are approved by the PSO which will include procedures for clearing of equipment, accessing of operators, clearing of media, handling malfunctions. GSSOs or CPSOs will position reproduction equipment to be continually monitored when it is outside a SAPF to achieve a risk mitigated solution. All reproduction equipment will be in compliance with applicable ISs guidance.

12. DESTRUCTION. Accountable SAP material will be destroyed using two SAP-briefed employees with access to the level of material being destroyed. Non-accountable SAP material may be destroyed by a single SAP-briefed employee with access to the level of material being destroyed. All classified waste containing SAP information will be destroyed as soon as possible. Such materials must not accumulate beyond 30 days unless approved by the PSO. NSA/CSS-approved equipment and their destruction procedures will be used to destroy SAP material as authorized by the PSO. Destruction of non-standard SAP materials will be approved by the PSO. Accountable and non-accountable SAP material will be maintained in accordance with the DoD Components record management manuals and instructions.

a. Prepare certificates of destruction itemizing each accountable document or material destroyed, to include citing the appropriate document control and copy number. For accountable

SAP material, destruction certificates must be completed and signed by both of the individuals involved in the destruction immediately after destruction is completed.

b. Public destruction facilities may be used only with the approval of and under conditions prescribed by the PSO.

# ENCLOSURE 6

# CYBERSECURITY

Reference (k) provides standardized cybersecurity related implementation guidance for policy and procedures for management of all networks, systems, and components at all classification levels for all DoD SAPs.

a. All DoD SAP ISs that receive, process, store, display, or transmit SAP information must operate in compliance this manual and References (h) and (k).

b. DoD SAP implementation of the Risk Management Framework, through the use of this manual, Annex B of Committee on National Security Systems Policy No. 22 (Reference (x)) and Reference (k) and in accordance with References (b) and (c), is aligned with Intelligence Community Directive Number 503 (Reference (y)).

c. Additional or compensatory technical and non-technical countermeasures may, after consultation with the Director of the CA SAPCO or designee, be imposed in the interest of SAP protection in coordination with the PSO.

# ENCLOSURE 7

# SETA PROGRAM

1. GENERAL. GSSOs or CPSOs will ensure that the SETA program meets the specific and unique requirements of this manual. The SETA program applies to all SAP-accessed individuals. General, non-SAP specific, or company-wide security briefings may be used to form the basis for or supplement the SAP SETA requirement. Training on the unique, SAP, and SAPF specific parameters of the SAP is required.

2. PSOs. PSOs will approve the SETA program of assigned SAPs. This may be a standalone document or incorporated into the SAPF's SOP.

3. GSSO(s) AND CPSO(s). GSSO(s) and CPSO(s) will:

a. Establish a SETA program for their SAP(s).

b. Annotate compliance with SETA requirements in the annual self-assessment checklist and provide to the responsible PSO in accordance with this volume.

4. ANNUAL TRAINING.

a. Activities that grant SAP access will ensure that accessed individuals receive annual training to reaffirm their responsibilities while accessed to a SAP. When major changes occur such as changes in the classification for information protected under a SAP, new SAP-specific information that requires protection will be updated in briefings and training.

b. Annual training by the PSO, GSSO, CPSO, or designee may take several different forms, to include but not limited to face-to-face briefings, computer-based presentations sent via e-mail on the appropriate classified network, single page data sheets requiring individual review and signature, or other methods as approved by the PSO.

(1) Annual training will be recorded by utilizing the SAP training record template posted on the DSS website at http://www.dss.mil/isp/specialprograms.html.

(2) If multiple SAPs are involved, a centralized record system may be utilized as approved by the PSO.

c. SAP-accessed individuals will be briefed by PSOs, GSSOs, and CPSOs on individual reporting requirements during initial briefings and during annual training in accordance with this manual.

# ENCLOSURE 8

# SECURITY INCIDENTS AND INQUIRIES

To ensure the protection of classified information to include classified information protected by SAPs, security incidents will be investigated and actions will be taken to ensure that the adverse effects of loss or compromise of classified information are mitigated. Security incidents involving classified information will be handled and investigated in accordance with this manual and References (b) and (u).

a. All security violations will be reported immediately, to the extent possible, and no later than 24 hours of discovery, to the PSO, through the procedures described in this enclosure.

b. The PSO, through the chain of command, will advise the CA SAPCO in all instances where national security concerns would impact any security program or personnel security clearances (PCL) of SAP-accessed individuals. The PSO will notify and report security violations to the GPM with a copy of the report to the appropriate CA SAPCO. The security official of the affected SAPF will recommend the scope of the corrective action taken in response to the violation and report it to the PSO for approval.

c. Actual or potential compromises involving DoD SAPs, the results of the compromise or inquiries, and investigations that indicate weaknesses or vulnerabilities in establishing SAP policy, or procedures that contributed to an actual or potential compromise will be reported to the CA SAPCO, Original Classification Authority, and the DoD SAPCO, who will report to the Director of Security Policy and Oversight, Office of the USD(I).

d. Personnel determined to have had unauthorized or inadvertent access to classified SAP information:

(1) Will be interviewed by the GSSO, CPSO, or PSO to determine the extent of the exposure.

(2) May be requested to complete an inadvertent disclosure statement. An inquiry will be conducted to determine the circumstances of the inadvertent disclosure.

e. Guard personnel or local emergency authorities (e.g., police, medical, fire) inadvertently exposed to SAP material during an emergency response situation will be interviewed by the GSSO, CPSO, or PSO to determine the extent of the exposure.

(1) The PSO will determine if an inquiry is required by Reference (u) to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information.

(2) The inquiry identifies the facts, characterizes the incident as an infraction or a violation, and identifies, if possible, the cause(s) and person(s) responsible, reports corrective action or a requirement for an investigation.

f. Refusal to sign an inadvertent disclosure statement by personnel inadvertently exposed to classified information will be reported by the GSSO or CPSO to the PSO by the next duty day.

# ENCLOSURE 9

# SAP COMPLIANCE INSPECTIONS

1. GENERAL. The SAP security compliance process represents a unified and streamlined approach to the SAP security compliance inspections. All SAPs will be subject to the security compliance inspection process. The detailed guidance, procedures, and Security Inspection Checklist for conducting security compliance inspections are posted on the website http://www.dss.mil/isp/specialprograms.html.

2. INSPECTION TYPES. Inspections are conducted to validate that SAP security processes and procedures are in compliance with the governing DoD policies and to ensure that the risk of compromise to SAP information is at a minimum. Inspections should be executed with the least amount of impact to the SAP, while maintaining a proficient, equitable, and comprehensive review.

a. There are four possible types of external inspections that can be conducted.

(1) Core compliance inspections will be conducted at the direction of the inspection official, at a minimum every 2 years. The core compliance inspection consists of:

(a) Self-inspection checklist

(b) Core functional areas (CFAs)

1. TS SAP data and materials accountability

2. SETA

3. Personnel security

4. Security management and oversight

5. Cybersecurity

6. Physical security

(c) Special emphasis items (SEIs)

(2) Full scope inspections require a 100 percent validation of all functional areas. A full scope inspection will be conducted at the direction of the CA SAPCO when a less than satisfactory overall rating has been received as a result of a core compliance inspection. The most serious security rating, an unsatisfactory rating, is assigned when circumstances and conditions indicate that the program management personnel within the SAPF have lost, or are in

danger of losing, their ability to adequately safeguard the classified material in their possession or to which they have access.

(3) Re-inspections are required when a less than satisfactory rating in one or more functional areas has been received. This can include just one or all functional area(s), SAP(s), or SEI(s). The re-inspection will be conducted no later than 90 days from the issuance of the final report.

(4) Unannounced or No Notice inspections can be full-scope or core compliance inspections conducted without notice and at the discretion of the CA SAPCO or designee.

b. A security representative from the prime contractor should be present and participate during inspections of subcontractors. Designated personnel will serve as inspection team chiefs, assign ratings, conduct in or out briefings, or be responsible for completing the security inspection report.

c. Inspections will be coordinated among the SAPCOs and DSS when not carved out and conducted jointly to the greatest extent possible. Compliance inspections involving multiple SAP organizations will be fully coordinated between participating DoD organizations by the assigned team chiefs. Each organization is responsible for publishing its report.

3. SELF-INSPECTION. Self-inspections are required to be conducted annually by the GSSO, CPSO or designee, for all SAPFs for which they are assigned responsibility. Utilize the security compliance inspection template and document any deficiencies in a corrective action plan that addresses the plan for correcting deficiencies and areas deemed unsatisfactory as noted in the report. All supporting information will be included in the self-inspection report.

a. The documented results of self-inspections will be retained until the next government inspection is completed. All outstanding items must be completed before the destruction of any compliance documentation.

b. The documented results of the self-inspections will be submitted to the PSO for coordination within 30 days of completion. The PSO will be notified immediately if the self-inspection discloses the loss, compromise, or suspected compromise of SAP information.

c. In addition to the CFAs, inspectors will be required to validate SEIs. The CA SAPCO will annually determine the SEIs and report to the DoD SAPCO. The CA SAPCO will provide input on the trends and recommendations of the prior year to the DoD SAPCO.

4. STAFF ASSISTANCE VISIT (SAV). During a SAV, the PSO or designee will review security documentation and provide assistance and direction as necessary.

a. SAVs should be conducted as required and may include:

(1) Self-inspection checklists and corrective action plans.

(2) Outstanding government action items.

(3) Administrative security documentation (i.e., SOP, CPSO and IA manager appointment letter, OPSEC plan).

(4) Violations and infractions.

(5) SAP-specific CI trends and briefings.

(6) SETA program.

(7) Physical security standards.

(8) Cybersecurity.

(9) TS accountability.

b. The PSO will provide a SAV report to the GSSO or CPSO detailing what was covered and identifying all actions requiring resolution. During this visit, the PSO will provide guidance and direction to the organization, which will assist in the development of an effective and standardized security program. The PSO will annotate and address any concerns that require follow up before the next inspection.

5. DEFICIENCIES. Once the inspection has been completed, the team chief will determine the rating of the inspection based on the number of deficiencies identified and the risk of a compromise to classified information. Deficiencies will be defined as a finding or deviation.

6. RATINGS. Inspection ratings are superior, commendable, satisfactory, marginal, and unsatisfactory.

a. If the rating is superior, commendable, or satisfactory, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days and place the organization on an inspection cycle not to exceed 24 months.

b. If the rating is marginal, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days and schedule a re-inspection on the marginal areas within 90 days.

c. If the rating is unsatisfactory, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 10 days and schedule a compliance security review to be conducted within 90 days.

# ENCLOSURE 10

# VISIT REQUEST PROCEDURES

1. GENERAL. Approval by the appropriate GPM or designated representative is required for all visits to SAP activities except for visits between the sites of a prime contractor and the prime's subcontractors, which may be approved by the CPM, or designee. A written or electronic visit notification must be approved before visiting a SAPF. Centralized personnel security databases may be used for access verification if authorized in writing by the responsible PSO or CA SAPCO, however GPM or designated representative approval of the visit is still required. All visit requests will be transmitted via PSO-approved channels.

2. ADVANCED NOTICE. SAP accessed personnel must make every effort to provide advance notification of the visit to their GSSO or CPSO. Visitors who courier classified material will provide travel itinerary, storage requirements, and emergency contact information to their GSSO or CPSO and the destination GSSO or CPSO.

3. UNANNOUNCED AND NON-VALIDATED ARRIVALS. Access will be denied if a visitor arrives at a government or contractor SAPF without verification of the requisite SAP accesses, except for the PSOs and supporting security staff members (as designated by the PSO) who may visit all SAPFs under their responsibility without furnishing advanced notification.

4. DURATION. Visit request authorizations in excess of 12 months are not permitted unless approved in writing by the PSO.

5. VALIDATION OF VISITOR'S IDENTIFICATION. The positive identification of each visitor will be made using an authorized credential in accordance with Directive-type Memorandum (DTM) 09-012 (Reference (z)); the identification number of the credential to be used will be annotated on the visit request. Federal Government-affiliated identification cards will not be used for positive identification in unacknowledged locations.

6. ESCORTING OF VISITORS.

a. Only resident SAP-accessed personnel can escort and closely control movement of non-SAP accessed visitors requiring access to a SAPF. The number of escorts required will be dependent upon the number of visitors and the capability of closely monitoring the visitor activities.

b. Foreign nationals visiting a SAPF will be approved by the CA SAPCO or designee.

c. The PSO or designee will determine whether an internal warning system (such as rotating light beacons) is necessary to warn accessed occupants of the presence of non-briefed personnel. The PSO or designee will employ other or additional methods (e.g., verbal announcements), as required, to warn or remind personnel of the presence of non-briefed personnel.

7. TERMINATION OR CANCELLATION OF A VISIT REQUEST. If a person is debriefed from the SAP before expiration of a visit request authorization, or if cancellation of a current visit request authorization is otherwise appropriate, the security officer or their designated representative will immediately notify all recipients of the cancellation or termination of the visit request authorization.

8. VISITOR RECORDS. Unless a PSO approved electronic visitor record is on file, the security officer will maintain segregated visitor logs for non-briefed and SAP accessed personnel. The visitor record will contain the visitor's:

a. First and last name.

b. Organization or firm.

c. Date visited.

d. Time in and out.

e. Sponsor.

f. Identification number of authorized credential in accordance with Reference (z).

g. Citizenship.

h. Purpose.

9. CONGRESSIONAL VISITS. The CA SAPCO will provide guidance when a congressional visit to a SAPF is proposed. In the event of the unannounced arrival of a congressional delegation, DoD employees accessed to DoD SAPs will contact the PSO for guidance. The PSO will contact the CA SAPCO for instructions. All communications and information flow between the authorized congressional members or their staff will be coordinated through the DoD SAPCO and CA SAPCO.

10. UNFORESEEN OPERATIONAL OR EMERGENCY SITUATIONS. When unforeseen events prevent providing a written or electronic visit notification, visit approval may be provided telephonically by the PSO or designee. Written certification and confirmation will follow verbal authorization within 24 hours.

ENCLOSURE 11

CONTRACTING

1. CONTRACT SECURITY CLASSIFICATION SPECIFICATION (DD FORM 254) REQUIREMENTS. The government contracting officer (GCO) awards contracts on behalf of the government and coordinates security requirements with the PSO. The PSO or designee prepares the DD Form 254. The GCO or designee signs as the certifying official for each prime contract. For subcontracts, the prime CPSO or designee prepares a DD Form 254 and forwards it to the PSO for review before release to subcontractors. Lengthy attachments to DD Form 254 that merely repeat information, policy, and procedures contained in any other security directives should not be included.

a. SAP security guidelines, in addition to all collateral and SCI requirements, will be provided in the DD Form 254.

b. The activity will notify the CA SAPCO if a government official imposes any security requirements exceeding those provided for in this manual. The activity will make the notification through the GCO who will generate a memorandum for signature by the CPM addressing the issues to the CA SAPCO.

2. CLEARANCE STATUS OF SUBCONTRACTORS. If a subcontractor does not have the requisite FCL, the prime CPSO or designee will submit a FCL request to DSS in accordance with Reference (e). Subcontractor personnel will have the appropriate PCL in accordance with Reference (e).

3. SECURITY AGREEMENTS AND BRIEFINGS.

a. A prime contractor is responsible for issuing contracts and entering into a formal relationship with the prospective subcontractor. The prime contractor will obtain approval from the PSO before any release of SAP information. When conducting business with non-SAP briefed subcontractors, prime contractors will ensure SAP information is not inadvertently released. Any relationship with a prospective subcontractor requires prior approval by the PSO. The PSO will ensure that the association with the government activity or any SAP capability is not disclosed.

b. Prior to the release of any SAP information, the prime contractor must brief any prospective subcontractor regarding the procurement's enhanced special security requirements. Arrangements for subcontractor SAP access will be pre-coordinated with the PSO. The CPSO will complete a subcontractor or supplier data sheet for submission to the PSO. Discussions with prospective subcontractors may occur provided the discussions are limited to general interest topics without association to the government agency and scope of effort. The CPSO will include the reason for considering a subcontractor and attaches a proposed DD Form 254 to the

subcontractor or supplier data sheet. The DD Form 254 will be tailored to be consistent with the proposed support being sought and be classified based on its content.

4. INDEPENDENT RESEARCH AND DEVELOPMENT (IR&D). The use of SAP information for a contractor IR&D effort occurs only with the specific written permission of the GCO. Procedures and requirements necessary for safeguarding SAP information is outlined in the DD Form 254 prepared by the PSO or designee. A letter defining the authority to conduct IR&D, a DD Form 254, and appropriate classification guidance will be provided to each contractor. Subcontracting of IR&D efforts will follow the same process as outlined in paragraph 1 of Enclosure 11 of this volume. IR&D operations and documentation that contain SAP information are subject to inspection in the same manner as other SAP classified information in the possession of the contractor.

5. FOCI. All SAP(s) follow established FOCI procedures outlined in Volume 3 of DoDM 5220.22 (Reference (aa)).

6. NATIONAL INTEREST DETERMINATION (NID). In accordance with section 2004.22 of Title 32, Code of Federal Regulation, (Reference (ab)) a NID is required before authorizing any contractor cleared or presently in process for an FCL under a special security agreement (SSA) access to SAP information or any other proscribed information. A NID does not authorize disclosure of SAP information to a foreign government, a non-U.S. citizen, or a non-U.S. entity. Approval of NIDs are based upon an assessment of whether the release of SAP information is consistent with the national security interests of the United States. The requirement for a NID applies to new contracts, including pre-contract activities in which access to proscribed information is required, and to existing contracts when contracts are acquired by foreign interests and an SSA is the proposed foreign ownership, control, or influence mitigation method.

7. DISPOSITION AND CLOSE-OUT ACTIONS.

a. CPSOs or designee will inventory, dispose of, request retention, or return for disposition all SAP material at contract completion or close-out. Request for proposals, solicitations, or bids and proposals contained in SAP files will be reviewed and screened by CPSOs in accordance with DoD Component records disposition instructions. Disposition of information by document control number will be submitted to the PSO and GCO for concurrence. Upon contract close-out, requests for retention of classified information will be submitted to the GCO through the PSO for review and approval. The contractor will not retain any SAP information unless specifically authorized in writing by the GCO. A final DD Form 254 will be issued for the storage and retention of SAP material. Storage and control requirements will be approved by the PSO.

b. At the initiation of a closeout, termination or completion of a contract, the CPSO will consider actions for disposition of residual hardware, software, documentation, SAPF, and

personnel accesses documented in a termination plan for approval by the PSO. The master classified material accountability record (log or register) will be transferred to the PSO at SAP closeout. All close out actions require final approval from the GCO and PSO.

# ENCLOSURE 12

# SAP TECHNOLOGY TRANSFERS

1. TECHNOLOGY TRANSFERS. Two primary issues must be addressed with all technology transfers. The first is to ensure that the scope of the gaining SAP SCG is sufficient to protect technology that is to be transferred. If not, the gaining SAP SCG must be updated (approved before transfer), or the transfer should not occur. The second issue is to ensure all technology to be transferred is reviewed to determine if there are any proprietary or data rights associated with the technology proposed for transfer. If so, those specific items must be clearly annotated with the appropriate data rights. The technology transfer agreement (TTA) is used to document transfers of SAP technology between U.S. government agencies. GPMs from both SAPs should maintain records of all technology transfers. TTAs can only be approved by the CA SAPCO or authorized designee. Transfers of SAP technology to a foreign government will be conducted in accordance with Foreign Disclosure Procedures in Reference (c).

2. SYSTEM OR CAPABILITY TRANSFERS. A system or capability transfer MOA will be prepared by the GPM, GSSO, and PSO for any system or capability transferred to or from a DoD Component from or to another DoD Component or non-DoD organization when the system or capability to be transferred requires continued resources to sustain. The system or capability transfer MOA must be approved by the CA SAPCO. The system or capability transfer MOA must include:

a. Description of technology to be transferred (i.e., data, knowledge, equipment).

b. Gaining and losing organizations.

c. Roles and responsibilities.

d. Gaining CSO.

e. Personnel security access requirements (if beyond standard requirements).

f. Logistics and sustainment requirements.

g. Marking guidelines and instructions.

h. Contracting review.

i. Legal review.

j. Resources necessary to sustain the SAP.

# GLOSSARY

## PART I. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| CA | Cognizant Authority |
| CFA | core functional area |
| CI | counterintelligence |
| CONUS | continental United States |
| CPM | contractor program manager |
| CPSO | contractor program security officer |
| CSO | cognizant security office |
| CUA | co-utilization agreement |
| DoDD | DoD Directive |
| DoDI | DoD Instruction |
| DoDM | DoD Manual |
| DSS | Defense Security Service |
| DTM | Directive-type memorandum |
| FCL | Facility Security Clearance |
| FOCI | foreign ownership, control, or influence |
| FOUO | for official use only |
| FWAC | fraud, waste, abuse, and corruption |
| GCO | government contracting officer |
| GPM | government program manager |
| GSSO | government special access program security officer |
| HVSACO | handle via special access channels only |
| IR&D | independent research and development |
| IS | information system |
| MOA | memorandum of agreement |
| NID | national interest determination |
| NISP | National Industrial Security Program |
| NSA/CSS | National Security Agency/Central Security Service |
| OA | oversight authority |
| OPSEC | operations security |
| PCL | personnel security clearance |
| PM | program manager |
| PPP | program protection plan |

| | |
|---|---|
| PSA | Principle Staff Assistant |
| RMF | Risk Management Framework |
| S | SECRET |
| SAP | special access program |
| SAPCO | special access program central office |
| SAPF | special access program facility |
| SAV | staff assistance visit |
| SCG | security classification guide |
| SCI | sensitive compartmented information |
| SEI | special emphasis item |
| SETA | security education and training awareness |
| SOP | standard operating procedure |
| SSA | special security agreement |
| TS | TOP SECRET |
| TSA | Transportation Security Administration |
| TSCO | TOP SECRET control officer |
| TTA | technology transfer agreement |
| USD(I) | Under Secretary of Defense for Intelligence |
| USG | U.S. Government |
| USPS | United States Postal Service |

## PART II. DEFINITIONS

These terms and their definitions are for the purposes of this volume.

authorization. The official management decision given by a senior organizational official to authorize operation of an IS and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the United States based on the implementation of an agreed-upon set of security controls.

carve-out. A provision approved by the Secretary or Deputy Secretary of Defense that relieves DSS of its NISP obligation to perform industrial security oversight functions for a DoD SAP.

commendable. A commendable rating is assigned to a contractor or government location that have fully implemented the security requirements in an effective fashion resulting in a commendable security posture, compared with other contractor or government locations of similar size and complexity. This rating denotes a security program with strong management support, the absence of any serious security issues, and minimal administrative findings.

compromise. The known or suspected exposure of classified information, clandestine activities, personnel operating under cover, or sensitive installations or assets to an unauthorized person(s).

corrective action plan. A document that addresses the plan for correcting deficiencies and areas deemed unsatisfactory as noted in the self-inspection report.

CPM. The individual responsible for management of SAP(s) at the contactor location.

CPSO. The individual designated in writing by the CPM who will provide security administration and management for a SAP at a cleared defense contractor location.

cryptographic ignition key. Device or electronic key to unlock the secure mode of cryptographic equipment.

CSO. Defined in Reference (g).

deviation. Undocumented procedures or deviations of approved processes that if left uncorrected could cause increased risk of loss or compromise of classified information. This could also include: Administrative issues that could result in multiple deviations; trends; or repeat deviations may result in a finding as they pertain to compliance inspections.

finding. A deficiency that could pose a direct impact to the integrity of the SAP. Security requirements that are missing or deficient that could result in a loss or compromise of classified information.

GCO. Any person who, by appointment in accordance with applicable regulations, has the authority to enter into and administer contracts and make determinations and findings with respect thereto. The term also includes the authorized representative of the contracting officer.

GPM. Also known as a commander or a director. The GPM is responsible for management of SAP(s).

GSSO. A government, or government support position, appointed in writing at a government SAPF or organization by the Director or PM to provide security administration and management. The GSSO receives SAP guidance from the PSO.

inadvertent disclosure. The involuntary unauthorized access to classified SAP or unclassified HVSACO information by an individual without SAP access authorization.

inquiry. An inquiry consists of fact-finding and analysis conducted to determine whether or not there was a loss of classified information or whether or not unauthorized personnel had, or could have had, access to the information. The inquiry identifies the facts, characterizes the incident as an infraction or a violation, and identifies, if possible, the cause(s) and person(s) responsible, reports corrective action or a more in-depth investigation. Inquiries, generally, are initiated and conducted at the lowest level possible.

inspection official. Government official with the authority to conduct SAP compliance inspections for government and industry within their agency or organization.

investigation. Conducted for a security violation when the incident cannot be resolved via inquiry or for incidents where an in-depth and comprehensive examination of the matter is appropriate.

loss. Occurs when classified information cannot be physically located or accounted for, such as classified information or equipment is discovered missing during an audit and cannot be immediately located.

marginal. A marginal rating indicates a substandard security compliance program. This rating signifies a serious finding in one or more security areas that could contribute to the eventual compromise of classified information if left uncorrected. The contractor or government location's size, extent of classified activity, and inherent nature of the problem, are considered before assigning this rating. A compliance security review is required within a specified period to assess the actions taken to correct the findings that led to the marginal rating.

mitigation measures. Equivalent protective measures used in lieu of implementing the exact wording of this volume of this manual. Equivalent levels of protection will not be designed with the intent to reduce or lessen the security requirements of this volume.

need-to-know. A determination that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

observation. A comment on any benchmark procedures, outstanding performers, or areas and processes that could be managed more effectively and not deficient on meeting any policy.

over flight. To fly over in an aircraft or spacecraft.

PSO. A government, or government support position appointed in writing by the appropriate Director CA SAPCO or designee, who is responsible for executing oversight and implementation of SAP security requirements for a specific SAP, group of SAPs or geographical assigned locations. The PSO is appointed to oversee and execute SAP security with responsibilities encompassing all security disciplines. The PSO exercises these responsibilities on behalf of the SAPCO.

requirements. Observations are made to identify options for the security compliance program and do not require a response or any actions to be taken.

risk management. The process that allows PSOs and security managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the systems and data that support their organizations' missions.

SAP Technology Transfer. The intentional communication (sharing) of SAP knowledge, expertise, facilities, equipment, and other resources for application to military and nonmilitary systems.

SAPF. A specific physical space that has been formally accredited in writing by the responsible PSO that satisfies the criteria for generating, safeguarding, handling, discussing, and storing classified or unclassified program information, hardware, and materials.

satisfactory. The most common rating which denotes that a contractor or government location's security compliance program is in general conformity with the basic requirements. This rating may be assigned even though there were findings in one or more of the security elements. Depending on the circumstances, a satisfactory rating can be assigned even if there were isolated serious findings during the security review.

self-inspection. A physical verification of the security processes, procedures, and administrative documentation that support the SAP.

superior. Reserved for a contractor or government location that has consistently and fully implemented the security requirements in an effective fashion resulting in a superior security posture, compared with other contractor government locations of similar size and complexity. The contractor or government location must have documented procedures that heighten the security awareness of the employees and that foster a spirit of cooperation within the security community. This rating requires a sustained high level of management support for the security program and the absence of any serious security issues. For more complex contractor government locations, minimal administrative findings are allowable.

unsatisfactory. Is assigned when circumstances and conditions indicate that the contractor or government location has lost, or is in imminent danger of losing, its ability to adequately safeguard the classified material in its possession or to which it has access. This rating is appropriate when the security review indicates that the contractor or government's security compliance program can no longer preclude the disclosure of classified information to unauthorized persons. When an unsatisfactory rating is assigned, a compliance security review must be conducted after a specified interval to assess the corrective actions taken before the contractor or government location's security rating can return to the satisfactory level.