DoD Manual 5205.07

Special Access Program Security Manual

Originating Component:	Office of the Under Secretary of Defense for Intelligence and Security
Effective:	January 17, 2025
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Manual 5205.07, Volume 1, "DoD Special Access Program (SAP) Security Manual: General Procedures," June 18, 2015, as amended
Incorporates and Cancels:	See Paragraph 1.2.
Approved by:	Milancy D. Harris, Acting Under Secretary of Defense for Intelligence and Security

Purpose: In accordance with the authority in DoD Directive (DoDD) 5143.01, this issuance assigns responsibilities and provides procedures to implement the policy established in DoDD 5205.07 and DoD Instruction (DoDI) 5205.11 for DoD special access programs (SAPs).

TABLE OF CONTENTS

TABLES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance 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 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 issuance as the "DoD Components").

b. All OSD and 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), memorandum of understanding, or other interagency agreement established with the DoD.

1.2. SUMMARY OF INCORPORATION AND CANCELLATION.

This issuance incorporates and cancels:

a. DoD Manual 5205.07, Volume 2, "Special Access Program (SAP) Security Manual: Personnel Vetting," November 24, 2015, as amended.

b. DoD Manual 5205.07, Volume 3, "Special Access Program (SAP) Security Manual: Physical Security," April 23, 2015, as amended.

c. Office of the Under Secretary of Defense for Intelligence and Security and DoD Special Access Program Central Office Memorandum, "Enrollment in Continuous Evaluation/Continuous Vetting as a Valid Prerequisite for Special Access Program Access," September 28, 2022.

d. Under Secretary of Defense for Intelligence and Security Memorandum, "Discussion, Handling, and Processing of Special Access Program Information in Accredited Sensitive Compartmented Information Facilities," November 21, 2023.

1.3. FORMS.

This issuance refers to forms managed or sponsored by the DoD. Unless otherwise mentioned in their citation, these forms are available at https://www.esd.whs.mil/Directives/forms/.

SECTION 2: RESPONSIBILITIES

2.1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

In addition to the responsibilities in Paragraph 2.6., the USD(I&S):

a. Establishes, develops, and coordinates DoD SAP security policy and provides security oversight in accordance with DoDDs 5143.01 and 5205.07.

b. Coordinates with the Director, DoD Special Access Program Central Office (SAPCO), and the Director, Defense Counterintelligence and Security Agency (DCSA), or other DoD adjudication facility, to obtain details informing access decisions regarding any condition, deviation, or waiver approved in accordance with the December 12, 2005 Office of Management and Budget Memorandum associated with an individual nominated for access to a DoD SAP.

c. May delegate approval authority for specific exceptions to policy.

2.2. DIRECTOR FOR DEFENSE INTELLIGENCE (COUNTERINTELLIGENCE, LAW ENFORCEMENT, AND SECURITY) (DDI(CL&S)).

Under the authority, direction, and control of the USD(I&S), the DDI(CL&S):

a. Develops policy in relation to, oversight of, and implementation of this issuance.

b. Processes requests for exceptions to the requirements of this issuance received from DoD SAPCO on behalf of the DoD Components and the Offices of the Principal Staff Assistants (PSAs) with cognizant authority (CA) over SAPs. Notifies DoD SAPCO of each approved exception.

2.3. DIRECTOR, DCSA.

Under the authority, direction, and control of the USD(I&S), the Director, DCSA:

a. Administers the National Industrial Security Program (NISP) for collateral classified requirements within the scope of contracts also involving SAPs in accordance with DoDI 5220.31 and Volume 1 of DoD Manual (DoDM) 5220.32.

b. In coordination with the DoD SAPCO, develops training for SAP security and administration professionals, implemented by CA SAPCOs, that adheres to the SAP security requirements in this issuance.

c. Develops and conducts SAP training, education, and certification in accordance with DoDD 5205.07 and DoDI 3305.13.

d. Oversees compliance with currently assigned industrial security requirements of defense contracts that require access to SAP information. No later than July 31, 2029, this responsibility will transfer to the CA responsible for the program.

e. Coordinates with the designated counterintelligence (CI) component to provide cross-sharing of threat and incident information affecting the security of the facility, defense information, or cleared personnel in accordance with Tables 1 through 4 of DoDI O-5240.10, when requested.

f. Conducts necessary investigative and adjudicative activities outlined in DoDI 5200.02 and DoDM 5200.02 for initial and continued eligibility to occupy a sensitive position or otherwise access classified information, suitability, or fitness for Federal employment for personnel nominate for or currently determined admissible to a DoD SAP.

g. No later than 180 days from approval of this issuance and in coordination with the DoD SAPCO Security Director, will complete creation of a SAP security role in Defense Information System for Security (DISS) and National Background Investigation Services. This role will be maintained for use as a primary vetting tool for SAP nomination process (SAPNP) eligibility determinations.

2.4. DIRECTOR, DOD SAPCO.

Under the authority, direction, and control of the Deputy Secretary of Defense (DepSecDef), the Director, DoD SAPCO:

a. Within 180 days from this issuance's effective date, will develop, in coordination with SAP Senior Working Group members as established in DoDD 5205.07, guidance to standardize the DoD approach to acquisition and management of SAP-protected intellectual property (IP), including patents, technical data, computer software, and associated license rights, as described in Section 3.

b. Serves as the DoD-designated original classification authority (OCA) for DoD SAP umbrella security classification guides (SCGs) on behalf of the Secretary of Defense (SecDef). See DoDM 5200.45 for guidance on OCAs and SCGs, Volume 1 of DoDM 5200.01 for information security requirements, and Volume 2 of DoDM 5200.01 for marking requirements.

c. Functions as the DoD single point of congressional liaison concerning SAPs and verifies that the congressional offices that are approved to process and store DoD SAP information implement the security requirements in this issuance.

d. Coordinates with the CA SAPCOs on SAP security matters, identifies trends, and makes SAP security policy recommendations to the USD(I&S).

e. Ensures the CA SAPCOs implement USD(I&S)-issued security policies and training requirements through the DoD SAP governance bodies established in DoDD 5205.07 and DoDI 5205.11.

f. In coordination with the USD(I&S), develops, maintains, and updates procedures for engagement with DCSA to request the adjudication service's rationale for approving any condition, deviation, or waiver associated with a nominated individual's clearance.

g. Supports the DCSA Center for the Development of Security Excellence in developing training for SAP security and administration professionals.

h. Develops, establishes, and maintains SAP facility (SAPF) accrediting official (SAPF-AO) training standards in coordination with the PSAs with CA over SAPs, the Director for National Intelligence, and the SAP security directors of the Military Services.

i. Develops and issues:

(1) The DoD SAP Enterprise SCG and Tier 1 umbrella SCGs.

(2) DoD-wide SAP inspection special emphasis items (SEIs).

j. Issues retention guidelines for SAP-related security documentation in accordance with DoDI 5015.02.

k. Develops, coordinates, and issues enterprise self-inspection documentation. Revised self-inspection documentation will be provided to DCSA for maximum awareness and availability.

l. Notifies the DDI(CL&S) of all exceptions established in accordance with Paragraph 2.1.c.

2.5. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In coordination with the Director, DoD SAPCO, and the USD(I&S), 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 DoDI 5205.11.

b. For information systems (ISs) that fall under DoD SAPCO cognizance, authorizes DoD SAP networks, databases, and ISs, including those that support SAP oversight and governance and delegates system owners in writing. For ISs that fall under the purview of the CA SAPCOs, delegates authorizing responsibility to the CA SAPCO and corresponding authorizing official (AO).

c. Plans and budgets for cybersecurity resources for SAPs under their purview.

d. Sets the baseline for cybersecurity requirements within the DoD SAP Enterprise, through the DoD Joint Special Access Program Security Implementation Guide (JSIG) or its successor. Maintains, annually reviews, and updates the DoD JSIG or its successor to require uniform, baseline security controls for confidentiality, integrity, and availability on DoD SAP IT that meet

or exceed all other applicable requirements for classified national security systems (NSS) in law, regulation, or USG policy.

e. Oversees complete and thorough tracking of SAP IT equipment in coordination with the CA SAPCOs.

f. Oversees and implements comprehensive cybersecurity strategies, including continuous monitoring, risk assessments, and incident responses, pursuant to Chapter 35 of Title 44, United States Code (U.S.C.).

g. Appoints an OSD or DoD-level AO to authorize SAP IS that process, store, or transmit OSD and DoD-level SAPs.

h. Maintains the system of record in a central database for all DoD SAP personnel and facility information.

i. Establishes and maintains a tool to consolidate and track SAP IT equipment.

j. Provide AO support for joint and enterprise level SAP systems. Define cybersecurity assessment and authorization support funding requirements for those SAP Enterprise or joint systems that are not directly funded by the DoD CIO.

k. Oversees compliance in IT investment management and review of and modification of IT projects based on performance pursuant to Chapter 113 of Title 40, U.S.C.

l. Follows requirements and procedures for NSSs as defined in Sections 3552(b)(6), 3553(e)(2), and 3553(e)(3) of Title 44, U.S.C., and established by the National Manager for NSS in accordance with National Security Directive 42, National Security Memorandum 8, and DoDD 5144.02.

2.6. DOD COMPONENT HEADS AND PSAS WITH CA OVER SAPS.

The DoD Component heads and PSAs with CA over SAPs:

a. Oversee their Component's implementation of this issuance.

b. Initiate actions to replace DCSA security cognizance activities, also known as "carve out," in accordance with DoDI 5205.11.

c. Notify DCSA of activities or areas for which DCSA is relieved from inspection authority.

d. Ensure that, as appropriate and in accordance with law and regulation, for all contractors who require access to DoD SAPs, the contract includes terms and conditions necessary to effectuate contractor compliance with all applicable responsibilities and procedures identified in this issuance.

e. Provide oversight, guidance, and administrative support to subordinate offices or activities related to DoD SAP policy and procedures in accordance with DoDD 5205.07, DoDI 5205.11, and this issuance.

f. Ensure complete and thorough accountability of SAP IT equipment.

g. In coordination with other stakeholders, develop SCG annexes for SAP compartments and sub-compartments for which the CA SAPCO is the primary stakeholder. If the CA has OCA delegated to it by position, the CA SAPCO will serve as the SCG annex OCA. If the CA SAPCO does not have delegated OCA, the CA SAPCO will utilize OCA within its chain of command in accordance with Volume 1 of DoDM 5200.01.

h. Coordinates with other stakeholders on the joint use of SAPs.

i. Ensure programs with CPI evaluate anti-tamper protections for CPI in accordance with DoDD 5200.47E and DoDI 5000.83.

SECTION 3: GENERAL PROVISIONS AND REQUIREMENTS

3.1. FUNCTIONAL ROLES AND RESPONSIBILITIES.

a. CA SAPCOs.

CA SAPCOs will:

(1) In coordination with DCSA, oversee their Component's continuing security awareness training and program requirements.

(2) Establish a SAP information security program to implement SAP accountability requirements and provide program security oversight and support in accordance with the requirements in this issuance.

(3) Implement and adhere to training guidelines issued by the DoD SAPCO and designate SAPF-AOs in writing.

(4) In coordination with the DoD SAPCO, submit requests for exception to any provisions of this issuance thru DDI(CL&S) for USD(I&S) decision. At a minimum, requests for an exception must include a risk assessment and operational requirements.

(5) Oversee SAP security, audit, compliance, cybersecurity activities, and reporting requirements for assigned SAPs and SAP accredited spaces.

(6) Designate personnel who may contact and provide information to and request information from the DoD Consolidated Adjudications Services and appoint SAP personnel vetting officials (SPOs).

(7) Evaluate information contained in a letter of compelling need (LOCN) to support access determinations for personnel nominated for DoD SAPs under their CA, or for which they are delegated access approval authority (AAA).

(8) Report any security issues that may result in the loss or compromise of SAP information to the DoD SAPCO within 48 hours. Security issues attributed to an individual will be reported to the applicable DoD adjudication authority.

(9) Ensure CI, law enforcement (LE), and security are integrated into risk management reviews of DoD SAPs.

(10) Develop and maintain a SCG annex for all content SAPs (See Paragraph 3.9.c. for additional information).

(11) Appoint CA SAPCO security directors who are in the 0080 Security Administration Series.

(12) Appoint an AAA.

(13) Protect all SAP systems and networks as NSSs in accordance with National Security Directive 42; National Security Memorandum 8; Sections 3552(b)(6), 3553(e)(2), and 3553(e)(3) of Title 44, U.S.C; and DoDD 5144.02.

(14) Oversee the integration of cybersecurity support within SAPs and subordinate tiers.

b. CA SAPCO Security Directors.

Security directors appointed by a CA SAPCO director:

(1) On behalf of the Component head, are responsible for implementation of security requirements of this issuance for all assigned SAPs and subordinate tiers, to include leading the Component's efforts to develop SCG annexes for each SAP in which the CA is a stakeholder.

(2) Oversee security management of subordinate offices and manage execution of all security policies and requirements for assigned SAPs in accordance with this issuance.

(3) Ensure that credible derogatory information is reported to the DoD Consolidated Adjudications Services.

(4) Oversee decisions to suspend, revoke, and reinstate SAP access for personnel and SAPs and subordinate tiers under their responsibility.

(5) Oversee, establish, and manage their Component's continuing security awareness training and program requirements to support the implementation of SAP security. Provide recommendations to the DoD SAPCO for training requirements and curriculum at the DCSA Center for Development of Security Excellence.

(6) Provide overall oversight and direction to program security managers (PSMs), program security officers (PSOs), SPOs, SAPF-AOs, government SAP security officers (GSSOs), and as appropriate, contractor SAP security officers (CSSOs).

(7) Formally appoint individuals to serve as SPOs, or delegate appointment authority in writing. Additionally, the security director may appoint GSSOs and approve appointment of CSSOs in organizations that do not have PSMs or PSOs to do this.

(8) Maintain a repository of all program protection plans (PPPs) under their cognizance, to ensure compliance with DoDI 5000.83 requirements. The PPP repository must be validated annually, at minimum.

(9) Ensure actions taken against an individual's SAP access are properly documented in the system of record and notifications are sent to DoD SAPCO to send actions to all DoD SAP security directors. Additional notifications must be made through collateral and sensitive compartmented information (SCI) security offices as appropriate.

(10) Approve technology transfer agreements on a case-by-case basis.

c. AAA.

The AAA:

(1) Makes SAP access approval or disapproval decisions, including evaluating a nominated individual's admissibility when a unique risk is identified.

(2) Coordinates with the SPO and the PSO, the government activity manager (GAM), the contractor activity manager (CAM), the supervisor, the commanding officer, or appropriate industry official to make informed decision on program access requests (PARs).

(3) Receives annual training on their authorities, standards, and limitations in accordance with CA SAPCO guidance.

d. GAM.

The GAM, as appointed by the CA SAPCO:

(1) Manages assigned SAP(s) and assumes the responsibility for overall security management of assigned SAPs.

(2) Coordinates with DoD CIO through their Component chief information officer and CA SAPCO, and with PSMs and PSOs to implement security, cybersecurity, program protection, and CI initiatives for critical technologies throughout the life cycle of a system, service, or critical technology.

(3) Allocates personnel, financial resources, and facilities to support SAP execution and maintain security compliance.

(4) Implements treaty and arms control measures, as applicable.

(5) Implements operations security (OPSEC) needed to support assigned SAPs.

(6) Ensures a tailored security education and training awareness (SETA) program for all personnel accessed to the assigned SAP.

(7) Coordinates with the resource authority and the information system security manager (ISSM) to:

(a) Plan and budget for program cybersecurity resources.

(b) Ensure compliance with established cybersecurity policy for all systems, including those under contract or vendor provided.

(c) Comply with all applicable cybersecurity and technology acquisition requirements, to include those set forth in DoDD 5000.01 and DoDI 5000.82 for all acquisitions including those for IS.

(d) Serve as the IS owner and ensure compliance with the DoD JSIG or its successor

(8) Plans and budgets for program security manpower resources, ensuring compliance with established SAP security policy for all operational locations, including those under support contract.

(9) In coordination with the PSM or PSO, reviews and endorses--annually, at minimum--all PPPs under their cognizance to ensure compliance with DoDI 5000.83 requirements. This includes ensuring the PSM or PSO provides a copy to the CA SAPCO security director, as required.

(10) Refers emerging technologies with potential for SAP protections, in accordance with Executive Order (E.O.) 13526 or any successor order, to the CA SAPCO for review.

(11) Maintains records of all technology transfers.

e. PSM and PSO.

(1) The PSM, as appointed by the CA SAPCO or designated security director:

(a) Manages the security oversight, guidance, and implementation of all insider threat, program protection, OPSEC, and security compliance activities for assigned SAPs (and any subordinate tiers or projects) employed across the joint force or interagency.

(b) Coordinates with the security director, GAM, and GSSOs to develop, implement, and enforce a security program that protects all facets of the assigned SAP compartments and sub-compartments to ensure security alignment and horizontal protections across the joint force and interagency.

(c) Assesses unique risks with all eligibility determinations granted with an exception code, unresolved derogatory information, or information derived from the pre-screening questionnaire (PSQ), and coordinates with the respective CI support activity, Insider Threat Cell. or the DoD Consolidated Adjudications Services, as necessary.

(d) Provides oversight and direction to PSOs, GSSOs, and, as appropriate, CSSOs to support assigned SAPs (or subordinate tiers or projects).

(e) Reviews the SAP nomination package and makes an access recommendation to the AAA.

(f) In coordination with the GAM, reviews and endorses--annually, at minimum--all PPPs under their cognizance to ensure compliance with DoDI 5000.83 requirements. This includes sending a copy to the CA SAPCO security director, as required.

(g) May perform PSO duties, as directed by the CA SAPCO or designated security director.

(h) Takes the appropriate security management office relationship in DISS, or successor system, to effectively manage individual personnel vetting information concerning an individual's eligibility for SAP access.

(i) Evaluates information developed from continuous vetting checks to ensure personnel continue to meet suitability for continued access to SAP.

(2) The PSO, as appointed by the CA SAPCO or designated security director:

(a) Is designated based on one of three categorizations: PSO, geographical PSO, or agency/organizational PSO.

1. The PSO exercises full-time responsibility for the overall security of their assigned SAP(s) implementing all security requirements and procedures prescribed in this issuance and other DoD security policy applicable to their program. Examples include:

a. Security oversight for SAP contracts.

b. On-site security support.

c. Protection of intelligence elements of an intelligence SAP.

d. Protection of structure or processes in an infrastructure program.

2. The geographical PSO:

a. Oversees SAP security activities within a geographical area.

b. Coordinates with the PSO to ensure security activities within a respective geographical area are conducted in accordance with this issuance, the relevant SCG(s) and SAP security guidance established by the PSM or PSO.

3. The agency/organizational PSO is appointed to a specific agency or organization to ensure security activities within a respective organization are conducted in accordance with this issuance, the relevant SCG(s) and SAP security guidance established by the PSM or PSO.

(b) Works with the GAM and GSSO to develop, implement, and enforce a security program that protects all facets of the assigned SAP compartments and sub-compartments.

(c) Provides security subject matter expertise to the GAM and GSSO and oversight of assigned SAP compartments and sub-compartments to ensure compliance with all established policy and procedures.

(d) Ensures the sufficient development and employment of SETA programs as described in Section 6.

(e) Oversees and works in tandem with GSSOs and CSSOs designated to support assigned SAP compartments and sub-compartments.

(f) Verifies annually that all SAPFs, as accredited by a CA SAPCO-approved SAPF-AO, are properly inspected for security compliance by:

1. Validating that each assigned GSSO and CSSO conducts and documents annual self-inspection and evaluates all inspection documentation in accordance with Section 8.

2. Approving the resultant corrective actions to establish or ensure compliance. Corrective actions will be reviewed every 30 days until all findings or deficiencies are satisfactorily addressed and approved by the PSO.

(g) Coordinates with IS AOs for ISs storing, processing, transmitting, and displaying special access required (SAR) information that the PSO is responsible for and applies risk management principles to SAP security architectures and environments.

1. Obtains threat and vulnerability information for identified assets and assesses the impact of potential attacks to determine the associated risk.

2. Assesses the vulnerability of critical program information (CPI), assets, or operations to specific threats.

3. Identifies risk mitigation measures, to include required costs and resources.

(h) In coordination with their SAP IS AO, approves changes to the IS security environment and operational needs that could affect the security authorization in accordance with the signed and approved authority to operate (ATO).

(i) During security compliance inspections, verifies that:

1. GSSOs and CSSOs are appointed in writing by the appropriate official, (i.e., by the commanding officer or GAM for GSSOs and by the CAM or appropriate industry official for a specific facility unit or location for CSSOs).

2. The GSSO or CSSO are routinely present to provide day-to-day security oversight in the facility or complex where the SAP work is conducted.

(j) Evaluates SPO's access eligibility recommendation and any additional information the nominated individual provides to "yes" answers on their PSQ.

(k) Assesses unique risks with all eligibility issues and coordinate with the respective CI support activity or the DoD Consolidated Adjudications Services, as necessary.

(l) Reviews the SAP nomination package and makes an access recommendation before forwarding it to the AAA for decision. If recommending the AAA non-concur, the PSM or PSO must provide additional justification in the PAR remarks section or in a separate memorandum.

(m) Ensures facility fraud, waste, abuse, and corruption (FWAC) information is prominently displayed.

(n) Appoints SPOs.

f. GSSO and CSSO.

(1) GSSOs and CSSOs will:

(a) Coordinate with the CA SAPCO, the PSM, the PSO, the GAM or the CAM, the commander, facility owner, or appropriate industry leader to create a secure environment to protect SAP information at each SAPF at a contractor location.

(b) Be responsible for security management, to include SETA, and related operations within their assigned activity, organization, or office.

(c) Implement and execute all SAP security requirements in this issuance, as well as any additional guidance issued by the CA SAPCO security director.

(d) Coordinate SAP security matters, including personnel vetting issues and security incidents, with the CA SAPCO, the PSM, the PSO, the GAM, or the CAM, as applicable, the commander, the facility owner, or appropriate industry leader, as well as ensure records are updated in the SAP personnel vetting system Joint Access Database Environment (JADE) or successor systems to ensure security professionals are aware of actions.

(e) Establish, conduct, and document initial, situational, and annual refresher training for all assigned SAP-accessed individuals.

(f) Conduct an annual self-inspection, document the self-inspection and any necessary corrective action plan, and submit the corrective action plan to the CA SAPCO PSM or PSO.

1. Before providing the corrective action plan to the PSM or PSO, the GSSO or the CSSO, will coordinate the self-inspection and proposed corrective action plan with organizational leadership for approval.

2. After submitting the leadership-approved corrective actions to the PSM or the PSO, provide updates to the PSM or the PSO every 30 days until all findings or deficiencies have been satisfactorily addressed and approved by the PSM or the PSO.

(g) Interface with SAP cybersecurity ISSMs to ensure the full protections of SAP material access is known, shared, and integrated into GSSO or CSSO, as applicable, and ISSM standard operating procedures (SOPs) to cover the full picture of SAP protection.

(h) Develop, maintain, and submit to the GAM or CAM, as applicable, for endorsement, all program protection implementation plans under their cognizance annually, at a minimum, to ensure compliance with DoDI 5000.83 requirements.

(2) GSSOs, as delegated by the PSM or PSO, will:

(a) Appoint SPOs. This authority may only be delegated to the GSSO if the PSM or the PSO has been delegated this authority by the CA SAPCO.

(b) Sign courier memorandums.

(c) Authorize and sign courier cards.

(d) Sign PAR PSO block when a nominee's PSQ contains all "no" answers.

g. SAPF-AO.

The CA SAPCO, or their designee in writing, will appoint in writing an individual to serve as SAPF-AO. The SAPF-AO is responsible for reviewing and approving or disapproving physical security preconstruction plans for, and physically inspecting and accrediting, reaccrediting, and de-accrediting, a SAPF. The SAPF-AO will provide SAPF accreditation-related actions to the GSSO or the CSSO, as applicable, to upload into the DoD system of record.

h. CAMs and Contractor Program Managers.

(1) CAMs are responsible for:

(a) Execution of and compliance with all applicable contractual performance requirements and other obligations to include security compliance.

(b) Reviewing all program protection implementation plans under their cognizance annually, at a minimum, to ensure compliance with DoDI 5800.83 requirements.

(2) Contractor program managers will appoint and submit, in writing for PSO consideration and approval, a CSSO to serve as the SAP security official at each contractor SAPF location.

i. SAP Accountability Officer.

The GAM or CAM will designate accountability officers in writing. When the PSO determines a program requires a SAP accountability officer, one will be appointed in writing by the GAM or the CAM.

(1) Accountability officers will account for all TOP SECRET (TS) SAR material, media, hardware, and equipment utilizing a CA SAPCO-approved accountability system. Accountability officers will account for all accountable SCI and collateral material, media, hardware, and equipment utilizing the same system.

(2) Accountability officers will account for all SECRET//SAR material, media, hardware, and equipment when directed by the CA SAPCO.

j. SPO.

The SPO will be responsible for the completeness and accuracy of information submitted in nominated individual's packages and make initial access determinations of recommendations in accordance with this issuance.

k. National Manager for NSSs.

In cooperation with the responsible CA SAPCO and the DoD CIO, the National Manager for NSSs has oversight of cybersecurity for all NSSs which include SAP networks.

3.2. SOPS.

a. The GSSO or the CSSO will prepare SOPs to implement the security policies and requirements applicable to their facilities, unit, organization or location, and the SAP(s) being executed therein. A single SOP can be written for a location with multiple SAPFs if any unique conditions or requirements for individual facilities are called out in the SOP, or a facility-specific appendix or annex to the SOP.

b. The GSSO or the CSSO will coordinate the proposed SOPs and SOP changes through organizational leadership before forwarding the proposed SOPs and SOP changes to the GAM or CAM, as applicable, for approval, if required by the CA SAPCO. After approval, the GAM or the CAM sends the document(s) to the PSM or PSO for policy compliance review and concurrence.

c. When a contractor is responding to a pre-solicitation activity, research and development announcement, request for proposal, or request for information, they will provide the government activity a description of the security processes and procedures that will be implemented to ensure only appropriately briefed personnel will have access to SAP information and material relevant to their response to the government.

d. CA SAPCOs will make SOP templates available to SAPs and subordinate tiers within their responsibility.

e. At a minimum, SOPs must include guidance on:

(1) General provision and requirements.

(2) Reporting requirements.

(3) Security clearances.

(4) SETA program.

(5) Visits and meetings.

(6) Subcontracting, as applicable.

(7) ISs.

(8) Sanitization, storage, and destruction.

(9) Reproduction procedures.

(10) Maintenance procedures.

3.3. FWAC.

a. Collateral FWAC reporting channels may not be used for FWAC complaints related to SAPs and subordinate tiers and information those protect.

b. Government and industry personnel will use only those FWAC reporting channels and phone numbers provided by the CA SAPCO security director.

c. PSM- or PSO-approved FWAC reporting information will be conspicuously posted in all SAPFs.

d. Individuals are not required to consult with or obtain approval from management before making FWAC reports.

3.4. OPSEC.

a. All SAPFs will have an OPSEC plan in accordance with DoDD 5205.02E. These OPSEC plans will be coordinated with the CA SAPCO or designated security director, must consider program-specific concerns, and be reviewed at least annually for updates.

b. OPSEC plans are also required for each SAP, subordinate tiers, or projects, which must be included within the establishment documentation. The OPSEC plans will be reviewed annually and updated at each lifecycle milestone or when missions dictate.

c. The OPSEC plans will include, as applicable:

(1) Related SAPs and subordinate tiers.

(2) Financial information.

(3) Manufacturing processes.

(4) Sub-contracting.

(5) Supply chain.

(6) Test and evaluation.

3.5. PPP.

a. All SAPs that manage activities to protect and enable technology innovation for present and future warfighting capabilities and programs will develop, implement, and maintain a PPP, informed by relevant science and technology protection plans and technology area protection plans, as appropriate, in accordance with DoDI 5000.83. They may also use alternative

documents that, when combined, meet the intent of the PPP. If a PPP would not be required for an equivalent non-SAP program, a PPP or set of alternative documents that when combined must:

(1) Identify CPI and critical components.

(2) Identify anticipated risks the program will encounter.

(3) Use threat intelligence from the Defense Intelligence Agency (DIA), DoD Component intelligence and CI activities, DCSA, or the Joint Acquisition Protection and Exploitation Cell.

(4) Incorporate information on foreign intelligence entity, cyber, and supply chain threats.

(5) Establish the CI support plan in accordance with DoDI O-5240.24.

(6) Establish a cybersecurity strategy.

(7) Address horizontal protection considerations for CPI and utilize the Acquisition Security Database as appropriate to track organic and inherited CPI eligible for anti-tamper.

(8) Have GAM and PSM or PSO endorsement.

(9) Complete an anti-tamper plan for all CPI identified.

b. PPPs will be reviewed annually, updated as needed to address current threats, validated with a signature by the GAM and PSM or PSO, and submitted to the CA SAPCO.

c. In coordination with the GAM, CAMs will submit a program protection implementation plan to the PSM or the PSO for all activities utilizing a SAP that is associated with a contract issued from a GCA.

3.6. CONSEQUENCE MANAGEMENT PLAN (CMP).

a. All capabilities or information protected by DoD SAPs that are fielded or deployed in a test or operational environment must have a CMP that establishes the plans and procedures for the recovery, reconstitution, and disposition or destruction of SAP-protected systems to account for a loss or suspected loss.

b. The PSM or the PSO and the GAM will coordinate CMPs with the appropriate DoD Component to sufficiently develop an integrated plan that will, at a minimum:

(1) Identify critical components and CPI.

(2) Provide guidance, describe general procedures, and identify coordination requirements for employment of the CMP.

(3) Assign general component levels tasks for the recovery, reconstitution and disposition, or destruction of SAP system to account for a mishap.

(4) Identify the specific operation or mission, to include scenario-based considerations that could lead to the use of the CMP.

(5) Establish a feasibility assessment, risk assessment, and concept of operations.

(6) Plan for control of public information release or distribution of video and images.

(7) If CPI utilizes anti-tamper protection, ensure the CMP includes notifying the Anti-Tamper Executive Agent or Component representative.

c. The CMP will be reviewed and updated annually and endorsed at a minimum by the GAM and the PSM or the PSO.

d. CA SAPCOs will ensure CMPs and their implementing procedures are established for the recovery, reconstitution, disposition, and destruction of SAP systems sold via foreign military sales. CA SAPCOs will coordinate CMPs associated with foreign military sales to oversight authority (OA) SAPCOs and DoD SAPCO.

3.7. IP STRATEGY AND PROCEDURES.

The OA or the CA SAPCO will develop procedures for reviewing patent applications involving SAPs consistent with DoDD 5535.02. The CA SAPCO and the OA SAPCO will coordinate with the Office of the DDI(CL&S) through the DoD SAPCO for patent security reviews for patent applications associated to subject inventions made in the performance of DoD contracts and government employee inventions.

3.8. ARMS CONTROL AGREEMENTS AND INTERNATIONAL LAW.

a. DoD SAPs must be protected against unauthorized or inadvertent disclosure during USG participation in authorized verification activities and confidence-building measures, such as overflights.

b. DoD will comply with applicable international law. However, the need to comply with an international organization does not, by itself, authorize exposing or revealing SAP information unless such measures are approved in accordance with this issuance. Additional guidance on arms control agreements can be found in DoDD 2060.01. Components will consult with their assigned Office of General Counsel and, as needed, with the DoD SAPCO.

3.9. SCGS.

SAP SCGs will be created, maintained, and updated in accordance with DoDD 5205.07, DoDI 5205.11, and DoDM 5200.45.

a. Enterprise SCG.

DoD SAPCO's Enterprise SCG, will:

(1) Introduce horizontal protection of DoD SAP information throughout the SAP Enterprise and architecture.

(2) Include standardized language applicable to all DoD SAP SCGs.

(3) Identify "Enterprise" processes and information that will be protected consistently across the SAP Enterprise (e.g., SAP nicknames, program identifiers (PIDs), and facts related to the number of people, and number of SAPs and subordinate tiers).

(4) Contain general administrative security classification guidance for all DoD SAPs.

b. Umbrella SCGs.

In collaboration with the CA SAPCOs, the DoD SAPCO will develop and publish one SCG for each SAP umbrella. Umbrella SCGs contain classification guidance for all SAP compartments or sub-compartments within the umbrella. The umbrella SCG will:

(1) Describe the umbrella-specific hierarchy of compartments and sub-compartments.

(2) Provide the scope of SAP protection specific to the umbrella.

(3) Provide broad descriptions and classification guidance for all CPI protected within the umbrella.

c. SCG Annexes.

CA SAPCOs, working collaboratively under the leadership of the office of primary responsibility (OPR) CA when there are multiple stakeholders, will develop one SCG annex for each content SAP compartment and sub-compartment in which the CA SAPCO is a stakeholder to identify CPI for the particular compartment or sub-compartment. SAP SCG annexes will contain security tables detailing the classification of specific CPI by reference to the umbrella SCG. SCG annexes will also contain other classification information that users will need to protect such information.

(1) SCG annexes will conform to Office of the USD(I&S) (OUSD(I&S)) guidance and will not exceed the scope or overarching classification guidance contained in the umbrella SCG. DoD SAPCO, in collaboration with the OUSD(I&S), will provide a template for SCG annexes.

(2) The OPR will lead development and maintenance of SCG annexes and collaboration among stakeholders for SAP compartment or sub-compartments with multiple stakeholders. Each OPR will determine and document the process for developing and updating SCG annexes the OPR deems most effective and efficient. DoD SAPCO will provide oversight of SCG annexes to ensure horizontal protection of CPI across the SAP Enterprise.

(3) The SCG annex cover page will list all stakeholders in the SAP compartment or sub-compartment.

(4) In signing and approving an SCG annex, the OPR CA or designated individual certify compliance with this section.

(5) The OPR CA or designated individual will submit the approved annex to DoD SAPCO.

(6) Upon receipt of a signed annex DoD SAPCO will:

(a) Annotate the SCG annex approval date in the umbrella SCG.

(b) Update the JADE, or any successor system, to reflect the action.

(c) Place the SCG annex into the appropriate DoD SAPCO-designated SAP SCG system of record.

(7) Stakeholders may request changes to an SCG annex through their CA SAPCO, who will coordinate with the OPR and other stakeholders to implement changes as needed.

3.10. 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 the appropriate CA SAPCO and DoD SAPCO.

(1) The DoD SAPCO will notify the designated focal point for the Office of the General Counsel of the Department of Defense of potential litigation involving SAPs at the earliest possible opportunity, not to exceed 48 hours after initial notification.

(2) CA SAPCOs will notify their designated legal counsel of potential litigation involving SAPs at the earliest possible opportunity, not to exceed 48 hours after initial notification. The designated legal counsel will notify the designated focal point for the Office of the General Counsel of the Department of Defense immediately upon receipt of such notification.

(3) These requirements apply to all legal or administrative actions in which the prime contractor, subcontractors, government organizations, or SAP-accessed individuals are a named party of the litigation, or are otherwise affected.

b. Individuals accessed to a SAP will immediately inform: (1) for government personnel, the PSM or the PSO, the GAM, the GSSO, or the commander/Director; or (2) for contractor personnel, the CAM, or appropriate industry official, of:

(1) Any litigation actions that may pertain to a SAP. PSMs or PSOs must also be notified of employee or union strikes, employer discrimination complaints, equal employment

opportunity cases, Merit Service Protection Board reconsiderations, litigation, etc., in accordance with the timelines required by DoDI 5205.11.

(2) Any event that could affect mission readiness, the safety and security of the facility, or cause a public disturbance. Notifications must also be made within 48 hours of becoming aware of allegations, investigations, or proceedings.

3.11. CI SUPPORT.

a. The organic CI entity or pertinent Military Department CI organization (MDCO) will assess foreign intelligence threats and risks to SAP information, material, personnel, systems, facilities (e.g., SAPF, destruction facilities), and activities in accordance with DoDD 5240.02 and DoDI O-5240.10. Information that may have a bearing on the foreign intelligence threat to a SAP or subordinate tier will be provided by the organic CI entity or pertinent MDCO to the affected GAM, PSM or PSO, commander, or appropriate industry official.

b. Contractors may request CI support to enhance or assist threat and risk planning and safeguarding in connection with contract performance. Requests for SAP-applicable CI support will be made to the respective PSM or PSO for approval before contractors receive such support.

c. Personnel will immediately report any attempt by unauthorized personnel to obtain SAP information to the PSM or the PSO and the GSSO or GAM, or CSSO, as applicable.

3.12. COMMUNICATIONS SECURITY.

a. SAP information will be electronically transmitted by approved secure communications systems in accordance with Committee on National Security Systems (CNSS) Instructions 5000 and 7003, and in an SOP approved by the PSM or PSO.

b. Voice and data communications will be on CNSS-compliant SAP IT systems approved for both the classification level of the information and for the SAP program(s) or subordinate tiers being transmitted on:

(1) A PSM- or PSO-approved communications device.

(2) On SAP or Intelligence Community (IC)-accredited SCI ISs or voice over internet protocol systems approved by the DoD SAPCO, the DoD CIO, or the CA SAPCOs.

3.13. INTERNATIONAL SAP SECURITY REQUIREMENTS.

Disclosure of DoD SAP-protected information and participation in SAPs with foreign governments will be approved by the SecDef or the DepSecDef, unless otherwise delegated.

a. Pre-release Procedures.

(1) SAP OA and CA requesting release of SAPs to foreign governments will work with the cognizant foreign disclosure offices to ensure that releasable core documents, as detailed in DoDI 5205.11, are available to the foreign governments within 30 days of foreign release approval.

(2) SAP OA and CA requesting release, in coordination with the SAP CA, will ensure the core documentation in accordance with DoDI 5205.11 is provided on an accredited SAP IT system to be shared with the foreign government.

(3) The Director, DoD SAPCO, in coordination with the requesting SAP OA or CA and applicable stakeholders, will identify the designated SAPCO (or organization with similar function) in the foreign government to ensure the necessary security procedures and associated documentation (e.g., foreign government PAR and SAP indoctrination agreement (SAPIA)) are developed and available for use to allow for timely exchange of SAP information.

b. Post-release Procedures.

(1) To access foreign nationals, the DoD Component will work with the Director, DoD SAPCO, to obtain PARs from the designated foreign SAPCO (or similar organization). PARs will be routed via JADE, or any successor system, using the same process as U.S. nominees. PARs must be signed by the foreign SAPCO or their designee before routing.

(2) Once foreign government PARs are approved, they will be sent via an accredited SAP IT system to the foreign SAPCO. Once the nominees are briefed, the foreign SAPCO will work with the Director, DoD SAPCO, to ensure the SAPIAs are archived in JADE, or any successor system. Foreign government personnel will sign their own national SAPIAs.

c. Visits and Assignments of Foreign Nationals Procedures.

(1) Visit certifications for U.S. DoD personnel traveling to a foreign nation will be forwarded by the cognizant security office to the Director, DoD SAPCO, via JADE, or any successor system, to the foreign SAPCO. The visit certification may also be sent directly to the foreign SAPCO, with a copy sent to the Director, DoD SAPCO.

(2) Visit certifications from the foreign SAPCOs will be forwarded to the Director, DoD SAPCO and uploaded to JADE, or any successor system, to the profiles of the associated foreign visitors.

(3) It is the responsibility of the cognizant security office to ensure all documentation is completed before travel.

(4) Consistent with DoDD 5230.20:

(a) Access for foreign liaison officers and cooperative program or project personnel, representing their foreign governments, will be accessed via the process outlined in Paragraph 3.13.b.(1).

(b) SAP eligibility and access for Defense Personnel Exchange Program (DPEP) that are assigned to the United States in accordance with DoDD 5230.20, will be processed via the Director, DoD SAPCO. The Director, DoD SAPCO, will validate eligibility via the DPEP's SAPCO organization (foreign SAPCO).

(c) Access for U.S. DPEP that are assigned overseas will meet the requirements outlined in Section 12 of this issuance. The Director, DoD SAPCO, will determine SAP eligibility in coordination with the cognizant security office.

d. Foreign SAPs Shared with the United States.

The Director, DoD SAPCO, serves as the OA for SAP protecting capability and information shared with the DoD by foreign SAPCO in accordance with DoDD 5205.07 and DoDI 5205.11, as well as delegated authorities provided by the foreign government releasing the SAP.

e. Security Incidents and Inquiries.

(1) All security incidents related to foreign SAPs released to the United States will be reported immediately, to the greatest extent possible, and no later than 24 hours of discovery, to the Director, DoD SAPCO, through the procedures described in Section 7 of this issuance.

(2) The Director, DoD SAPCO, in coordination with the DoD Component reporting the incident, will provide reporting to the respective foreign government SAPCO.

f. Other Matters.

(1) The Director, DoD SAPCO, will document processes to monitor billet access quotas, status of core documentation, and other security related matters in coordination with the appropriate CA SAPCOs, OAs, and cognizant disclosure offices.

(2) SAP reciprocity, including but not limited to physical security, IT, and personnel vetting will be subject to separate arrangements between the Director, DoD SAPCO, and the foreign governments, in accordance with DoD policies.

(3) Additional security requirements are further identified in bilateral program-specific security agreements, general security of military information agreements, and industrial security agreements.

3.14. RECORDS MANAGEMENT.

SAP records must be managed in accordance with the OSD Records Disposition Schedule. Records created during SAP execution and oversight are managed in compliance with DoDI 5015.02, and IT capabilities supporting the oversight are compliant with DoDM 8180.01 and Directive-type Memorandum 22-001.

SECTION 4: SAFEGUARDING CLASSIFIED INFORMATION

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

a. HVSACO Usage.

(1) HVSACO is a control marking, and it is not a classification level or dissemination control. In accordance with Volume 2 of DoDM 5200.01, HVSACO is applied to non-SAP material (unclassified or classified) that exists within a SAP environment and, due to its subject or content, warrants handling only within SAP channels among SAP-cleared personnel. The term "SAP channel" denotes approved SAP communications systems, accredited SAPFs, or otherwise approved SAP storage areas. Information may only be designated with the "HVSACO" handling instruction by an OCA, as codified in the SAP Enterprise or an umbrella SCG. The highest marking for PIDs and program names is controlled unclassified information (CUI). The HVSACO handling caveat is not authorized for PIDs and program names without a waiver and approval by the CA SAPCO.

(2) In accordance with Volume 2 of DoDM 5200.01, SAP information will be marked in accordance with the SCG. HVSACO will not be used in lieu of any defined classification codified within an SCG. If questions on marking guidance arise, the guidance in the SCG takes precedence.

(3) HVSACO will be retained within SAP-approved channels, and dissemination of HVSACO information will be limited to persons briefed to at least one DoD SAP or another SAP belonging to another department or agency authorized to establish and maintain SAPs in accordance with Section 4.3. of E.O. 13526 or any successor E.O.s. This includes personnel with access to Office of the Director of National Intelligence (ODNI) controlled access programs (CAPs).

(4) Additional PARs or SAPIAs will not be used for access to HVSACO material.

(5) Examples of HVSACO-eligible information, which may be supplemented by additional guidance in a DoD SAPCO-issued Enterprise SCG, include:

(a) When necessary to protect sensitive relationships between non-program information and program CPI.

(b) To protect information that does not warrant classification under E.O. 13526, or any successor orders, and when determined in writing by the Director, DoD SAPCO, that controlling the information as CUI in accordance with E.O. 13556, or any successor E.O.s, is insufficient.

(6) HVSACO impedes interagency collaboration and SAP-level integration. To mitigate that risk and support the need for collaboration and integration:

(a) DoD SAPCO may administratively remove HVSACO or establish criteria for reciprocity for HVSACO-marked information for the purpose of collaboration and integration, with prior notification to CA SAPCOs.

(b) Personnel read into at least one SAP and, with a demonstrated need to know (NTK) (including ODNI CAPs and other USG SAPs as allowed by E.O. 13526 or any successor E.O.s), may use and access the HVSACO marking and information it controls. This includes personnel with access to SCI.

(c) ISs approved to hold SAP information, including approval to hold ODNI CAPs and other USG SAPs as allowed by E.O. 13526 or successor E.O.s, may hold, process, and display HVSACO-controlled information. If those ISs do not use the HVSACO marking itself, they may indicate the presence of HVSACO information by use of a clearly seen warning statement (e.g., "This document contains HVSACO information") instead of incorporating the marking into the banner lines and portion markings themselves.

b. Training and Procedures.

Training on HVSACO will be included in initial training or indoctrination and annual security awareness refresher sessions. Procedures for the use of HVSACO must be included in the SAP Enterprise or umbrella SCGs.

c. HVSACO Storage.

HVSACO material must be stored in an accredited SAPF or sensitive compartmented information facility (SCIF) or other area approved by the PSM or the PSO, for storage. HVSACO may be openly stored if authorized in writing by the PSM or the PSO.

d. Transmission of HVSACO Material.

(1) HVSACO-protected material is not approved for transmission via unclassified or collateral networks or telephones. Transmissions of this type constitute a security violation and an inquiry or investigation must be completed in accordance with Volume 3 of DoDM 5200.01.

(2) HVSACO material and information may be:

(a) Electronically transmitted on approved networks and ISs. Before including SAP information on the network, verify if the network or IS are approved to process.

(b) Sent via United States Postal Service (USPS) First-Class Mail. Refer to Volume 3 of DoDM 5200.01 for guidance on mailing classified HVSACO information.

(c) Transmitted via PSM- or PSO-approved secure fax machines.

(d) Discussed on a telephone system approved for SAP or SCI discussion (e.g., a National Secure Telephone System phone (commonly known as a "JWICS phone" or "TSVOIP phone").

e. Reproduction of HVSACO Material.

Reproduce HVSACO-protected information only on equipment authorized for SAP reproduction.

f. Accountability and Destruction.

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, and internal or external transmission and destruction receipts are not required for unclassified HVSACO.

g. Reporting Requirements.

For suspected security violations involving HVSACO-protected information, regardless of classification, notify the local SAP security representatives (GSSO or CSSO) immediately to ensure the PSM or PSO is notified within 24 hours of discovery. The PSM or PSO, in coordination with the GSSO or the CSSO, the GAM or the CAM, the commander, or appropriate industry official, will conduct a preliminary inquiry and will determine if a violation will result in suspended or revocation of program access. Violations will be reported to the CA SAPCO.

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

a. Secure Encryption Devices.

(1) All encryption devices used for the secure communication or electronic transmission of SAP information or data will meet CNSS guidance for National Security Agency/Central Security Service (NSA/CSS)-approved encryption technologies for NSSs.

(2) Secure faxes may be used for the transmission of SAP information on PSM- or PSO-approved devices. Procedures for use of these devices will be documented in the SOP. Unless approved by the PSM or PSO, auto-polling functions are not authorized for use.

(3) All equipment used for the voice over internet protocol, video teleconferencing electronic transmission of SAP information must be approved by a CA SAPCO AO, and procedures for their use documented in the SOP.

b. Electronic Transmission.

(1) When using electronic transmission, to include voice over internet protocol, video teleconferencing for SAP material, encrypted communications equipment identified in Paragraph 4.2.a.(1) will be used.

(2) When secure electronic transmission is permitted using a system with a valid ATO, the CA SAPCO AO, in coordination with the PSM or PSO, will notify the GSSO or CSSO of the system approval in writing.

4.3. ACCOUNTABILITY.

a. An accountability system approved by the CA SAPCO or written designee will be developed and maintained for SAP and non-SAP classified information subject to accountability requirements. The accountability system must:

(1) Clearly detail what information is accountable and non-accountable.

(2) Incorporate accountability requirements for TS information.

(3) Cover all TS//SAR material, media, hardware, equipment, etc.

(4) Cover SECRET//SAR material, media, hardware, equipment, etc., when directed by the CA SAPCO.

(5) Document all IT hardware, equipment, and media entering and exiting a SAPF.

(6) Include additional items subject to accountability when directed by the CA SAPCO.

(7) Incorporate DoD watermarking requirements for all printed TS information in accordance with April 16, 2024 Acting USD(I&S) memorandum.

(8) Generate inventory reports and tailorable inventory schedules.

(9) Generate hand receipts and sub-hand receipts.

b. The accountability system will record all transactions of handling, receipt, generation, reproduction, dispatch, or destruction and assign individual responsibility for all accountable information not residing on a SAP-accredited IS. An automated system, if used, must have a backup. When SAP material is received with the originator's accountability control number, the recipient's accountability system will include the originator's accountability control number.

c. At a minimum, accountability systems must include:

(1) Classification, dissemination controls, or CUI designation.

(2) Program nickname or PID, if SAP is from the DoD, IC CAP, or another department or agency.

(3) Originator of the item.

(4) Title and description of item.

(5) Custodian assigned.

(6) Date of product.

(7) Control number.

(8) Copy number.

(9) Page count.

(10) Disposition and date.

(11) Destruction date.

(12) Internal and external receipt records.

(13) Secure storage location.

(14) Accountable individual (i.e. receipt holder) or entity.

d. The CA SAPCO, or their designee in writing, will maintain a disclosure sheet for all TS//SAR items, regardless of format. The individual's name is recorded only once regardless of the number of times subsequent access, as defined in E.O. 13526 or successor order(s), occurs.

(1) Movement of SAP classified material, hardware, equipment, and all media will be in compliance with the DoD JSIG or its successor.

(2) Once destruction of an accountable item takes place, the disclosure sheet will be kept with the destruction paperwork and destroyed in accordance with the applicable records disposition schedule after the item is destroyed.

e. Electronic files do not need to be placed into accountability systems or the information management system referenced in Paragraph 4.4.a. when residing on an IS. They also do not require receipts when transmitted electronically.

f. TS accountability will implement guidance in the April 16, 2024 Acting USD(I&S) Memorandum, and include:

(1) Expanded use of "I agree" accountability attestations, which users must click on to affirm their understanding of security requirements for the information they are accessing.

(2) Implementing local or system level access controls on networks and shared drives with TS information.

(3) Inclusion of a standard timeline within the SAP SOP, not to exceed 3 months, whereby user accounts on TS networks that have not logged in are suspended.

(4) Watermarking program and non-program printed TS material. All media, regardless of classification, is subject to control. Media will be recorded in a log, receive a tracking number (separate from the accountability number), be tracked when going in or out of the SAPF, and be inventoried annually. Procedures for control of media should be included in the SAPF SOP and need not direct the use of the CA SAPCO's designated accountability system.

4.4. ANNUAL INVENTORY.

a. A complete and thorough, 100 percent, inventory of accountable SAP and non-SAP material and equipment will be conducted annually by the individual responsible for the control system or their alternate and a disinterested party. All inventory reports will be made available during security compliance inspections in accordance with Section 8 of this issuance.

(1) When an organization has a high volume of SAP materials, CA SAPCOs may request in writing, and DoD SAPCO may approve, a representative percentage of the total accountable holdings to be inventoried. The CA SAPCO request must provide a rationale, describe how it will manage risk without conducting the complete inventory requirement, and state discovery of missing information will result in revocation for those culpable.

(2) The annual inventory date will not exceed the previous year's inventory date by more than 365 days.

(3) Inventories will be conducted by visual inspection of all items of accountable material and verification of pertinent information, including originator, date, subject, file number, and page count for TS//SAR documents held within the SAPF.

(4) PSMs and PSOs may approve alternate processes or procedures for verifying accountable items when verification of pertinent information is not feasible due to operational requirements. Any such alternate method must be documented and reported to the CA SAPCO or designee security director.

b. Discrepancies between accountability records and annual inventories must be reported immediately to the GSSO or the CSSO, who then report to the PSM or the PSO. The PSM or the PSO will ensure action is taken, as appropriate, in accordance with Section 8.

c. As part of the annual inventory, the continued need for all accountable items will be assessed and non-record items no longer required will be destroyed in accordance with Paragraph 4.9.

d. Any collateral contract information incorporated into an acknowledged SAP, including accountable non-SAP information, must be listed on the DD Form 254, "Department of Defense Contract Security Classification Specification," or approved by the PSM or PSO before entry.

4.5. TRANSMISSION AND PREPARATION OF SAP-CLASSIFIED MATERIAL.

a. General Procedures.

(1) SAP information may only be transmitted outside SAPFs using one of the methods identified within this section, and the GSSO or CSSO will oversee compliance with these requirements. The order of precedence for transmission processes is:

(a) ISs that include a secure controlled interface that meets prescribed security configuration controls.

(b) Courier, to include use of diplomatic pouch.

(c) PSM- or PSO-approved government or commercial carrier for SECRET//SAR and CONFIDENTIAL//SAR material.

(d) Defense Courier Division or other documented PSM or PSO approval for TS//SAR material.

(e) USPS registered mail for SECRET//SAR and CONFIDENTIAL//SAR material within the contiguous United States, when approved by the PSM or the PSO. When associations present an OPSEC concern in receiving and sending mail, the GSSO or the CSSO will coordinate with the PSM or the PSO on developing an OPSEC appropriate countermeasure.

1. USPS registered mail for SECRET//SAR material.

2. USPS certified mail for CONFIDENTIAL SAP.

3. USPS First Class mail for CUI and unclassified HVSACO material.

(2) Packages using a USG-approved contract carrier (i.e., USPS Express Mail) transporting SAP information approved by the PSM or PSO for that delivery method may only be shipped on Monday through Thursday, and the expected delivery date must be checked to ensure that the carrier does not retain the classified package over a holiday or weekend.

(3) The methods of transmitting selected SAP information in Paragraph 4.5.a.(1) 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.

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

(a) Written approval is received by the PSM or the PSO.

(b) SAP requirements dictate.

(c) It is essential to mission accomplishment.

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

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

(5) To ensure direct delivery to address provided by the PSM or the PSO:

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

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

b. Package Preparation and Handling.

Package SAP information or other material in accordance with Volume 3 of DoDM 5200.01.

c. Courier Guidance.

SAP material will be transported in accordance with the transportation plan from one SAP-accredited facility to another in a secure manner that is not obvious and does not attract attention. The GSSO or the CSSO, or authorized designee, will provide detailed courier instructions and training to SAP-briefed couriers when hand-carrying SAP information. Problems encountered will be reported immediately to the PSM or PSO, who may authorize exceptions when operational considerations or emergency situations dictate. The following rules will be adhered to when couriering SAP material:

(1) Courier(s) must be accessed to the SAP(s), unless authorized by the CA SAPCO or designee.

(2) Courier(s) must make every effort to provide advanced notice to their GSSO or CSSO and the destination GSSO or CSSO and share a copy of their travel itinerary, storage requirements, and emergency contact information as part of their notice. At a minimum, the travel itinerary will be safeguarded as CUI to protect OPSEC critical information and indicators.

(3) For local travel, non-accountable SAP material may be hand-carried by a single courier using a locked courier pouch as the outer wrapper. The key must be removed and stowed separately from the pouch.

(a) Local travel will be defined by the CA SAPCO or designee.

(b) Travel outside of the defined local area of the originating SAPF requires PSM or PSO approval.

(c) The locked courier pouch must have a tag or label with the courier's full name, organization, and telephone number.

(4) Travel should be performed using a company-owned, rented, personally owned, or government vehicle. Use of public transportation or ride share services requires PSM or PSO approval.

(5) Couriering TS//SAR requires two-person integrity. The PSO or the PSM may approve documented exceptions on a case-by-case basis.

(6) A single-person courier may be used for SECRET//SAR and below materials.

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

(8) At a minimum, the GSSO or CSSO from the courier's departure location will provide each authorized courier with a copy of DD Form 2501, "Courier Authorization," or a PSM- or PSO-approved, locally produced courier authorization memorandum.

(9) At a minimum, the courier authorization memorandum will address and include:

(a) Method of transportation.

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

(c) Completion of receipts, as necessary, and unclassified description of the classified data being transferred.

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

(e) A place for the courier to sign, acknowledging their courier requirements.

(10) 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 CSSO, for ground couriering, instead of individual letters for each trip. A hand carry authorization memorandum is required for all air travel. The DD Form 2501 is issued and revalidated in accordance with Volume 3 of DoDM 5200.01.

d. Transportation Plans.

(1) The GSSO or CSSO will develop a transportation plan coordinated with and approved by the PSM or PSO before the proposed movement of any SAP material(s). The facility's SOP will include procedures for:

(a) Transfer of SAP material by courier within the local area, as approved by the PSM or PSO.

(b) Reoccurring transfers (e.g., weekly or monthly).

(2) For transport of material unable to be hand carried by a courier (e.g., bulky or heavy classified equipment, large quantity of documents), the GSSO or CSSO will develop a transportation plan coordinated with and approved by the PSM or PSO in advance of the proposed movement. The intent is to provide the PSM or PSO with reasonable time to meet operational necessity. 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 (e.g., 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, including a description of emergency procedures and who is responsible for actions that must be taken in the event of an emergency, e.g., an unexpected stop anywhere along the route. Identify individuals by name, and provide their organization, telephone, and e-mail addresses. Fax numbers may also be included.

(e) Ensure CI support is incorporated into transportation planning and execution, as approved by the PSO or PSM.

4.6. AIRPORT SCREENING GUIDELINES FOR CLASSIFIED MATERIAL.

a. Transportation Security Administration Guidelines.

Transport classified information or other material during air travel in accordance with Volume 3 of DoDM 5200.01.

b. Travel to or From Locations Outside the United States.

(1) Classified information will be sent via secure classified SAP IS whenever possible. Classified fax using SAP-authorized equipment may also be used.

(2) Use of Diplomatic Courier Service via diplomatic pouch is required for transport of SAP material outside the United States.

(3) If a diplomatic pouch is not available, hand-carrying classified SAP material overseas requires approval from the CA SAPCO or designee.

(4) Once overseas, use of a government or official vehicle is required, unless approved by CA SAPCO or designee.

4.7. REVIEW AND RELEASE OF INFORMATION.

a. Public release of SAP information is not authorized without written approval from the SecDef or DepSecDef and notification of the appropriate congressional committees in accordance with Section 119 of Title 10, U.S.C., and Sections 2011 through 2259 of Title 42, U.S.C. Only the SecDef and the DepSecDef can authorize public release of SAP information.

(1) Classified or sensitive information concerning SAPs may not be included in unauthorized government or non-government publications, technical review documents, or marketing literature.

(2) All material proposed for release will be submitted through the PSM or the PSO to the GAM at least 60 days before the proposed release date.

(a) The PSM or the PSO will notify the CA SAPCO or designee security director of any request involving SAP material.

(b) The PSM or the PSO will submit any non-SAP for prepublication review in accordance with DoDIs 5230.09 and 5230.29. Additional information about security review and public release is found at https://www.esd.whs.mil/DOPSR/.

(c) If approval is granted, additional case-by-case requests to release identical, previously approved information are not required.

b. Personnel currently or previously accessed to a SAP will, before public release, send a copy of any proposed publication, written material, briefings, or other prepared remarks intended for release that could potentially contain SAP information to the GSSO or the CSSO for PSM or PSO and GAM review and approval.

(1) 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 CA SAPCOs with equity before release, who will coordinate with other DoD Components based on their chartered responsibilities.

(2) The information and materials proposed for release will remain within SAP security channels until authorized for release.

c. Each GSSO or CSSO 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.

d. Public requests for SAP information will be processed pursuant to Section 552 of Title 5, U.S.C. (also known and referred to in this issuance as the "Freedom of Information Act"), and DoDD 5400.07.

4.8. REPRODUCTION.

a. SAP information will only be reproduced, including print-only, on networked or stand-alone equipment approved by the PSM or the PSO.

(1) The GSSOs or the CSSOs will include reproduction procedures in their facility's SOP.

(2) Clear markings will be used to indicate whether equipment can or cannot be used for reproduction of SAP material, as well as the level of classification that can be reproduced. This includes General Services Administration-approved media labels.

b. 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 designated solely for maintenance purposes should be purchased.

c. Reproduction equipment may only be used in a SAP working area (SAPWA) or SAP temporary secure working area (SAPTSWA) when it can be continuously monitored and with the documented approval of the PSM or the PSO or according to PSM- or PSO-issued written procedures. At a minimum, the written procedures will include the processes for:

(1) Accessing operators.

(2) Clearing media.

(3) Clearing equipment.

(4) Correct handling of malfunctions.

(5) Destruction of material if equipment cannot be cleared.

d. All reproduction equipment will comply with the DoD JSIG or its successor guidance.

e. Disposition of reproduction equipment that is replaced or taken out of service will be handled in accordance with CA SAPCO-approved equipment lifecycle management SOPs and destruction procedures in Paragraph 4.9.

4.9. DESTRUCTION.

At a minimum, SAP material must only be destroyed using approved destruction methods and processes in accordance with this issuance. These processes may be subject to additional guidance by the CA SAPCO and PSM or PSOs.

a. Accountable SAP material will be destroyed by two SAP-briefed personnel with access to both the classification level and each SAP included in material being destroyed, except as provided for in Paragraph 4.9.f. or as authorized by the CA SAPCO. SAP material can be destroyed by methods in NSA/CSS Policy Manual 9-12 or the April 20, 2020 DoD CIO Memorandum.

b. Non-accountable SAP material may be destroyed by a single SAP-briefed employee with access to both the classification level and each SAP included in material being destroyed. SAP material can be destroyed by methods in NSA/CSS Policy Manual 9-12 or the April 20, 2020 DoD CIO Memorandum.

c. All waste containing or revealing SAP information will be destroyed as soon as possible. Such materials must not accumulate beyond 30 days unless approved by the PSM or the PSO. The CA SAPCO, or their designee in writing, will be coordinated with and approve all destruction of accountable material.

d. NSA/CSS-approved equipment and their destruction procedures will be used to destroy SAP material and any equipment containing SAP material in accordance with approved records schedules.

(1) Destruction of non-standard SAP materials will be approved by the PSM or the PSO.

(2) Destruction certificates must be completed for all accountable SAP material destroyed and will be signed by both authorized personnel involved in the destruction immediately after destruction is completed. The destruction certificates will:

(a) Itemize each accountable document or material destroyed and include citation of the appropriate document control and copy number.

(b) Be made available to the CA SAPCO, or their designee upon request.

(c) Be maintained in accordance with the approved records schedule.

e. Commercial destruction facilities or services are authorized for use only with the approval of and under conditions prescribed by the CA SAPCO or designee and under conditions no less restrictive than for the destruction of TS/SCI materials.

f. Destruction of SAP IT equipment will be conducted in accordance with supplemental guidance provided by the DoD SAPCO, in coordination with the DDI(CL&S) and the Deputy Chief Information Officer (DCIO) for SAP IT.

4.10. CLASSIFIED MARKING REQUIREMENTS.

a. Marking of SAP classified information will follow Volume 2 of DoDM 5200.01.

b. Exceptions to this requirement may be approved by the CA SAPCO in a fully subscribed OPSEC plan, accomplished in accordance with Paragraph 3.4. Approved exceptions will be reported to the USD(I&S) through the DoD SAPCO as part of the annual SAP reviews conducted in accordance with DoDD 5205.07.

SECTION 5: CYBERSECURITY

DoD JSIG or its successor provides standardized cybersecurity-related implementation guidance for policy and procedures regarding management of networks, systems, and components for DoD SAPs.

a. All DoD SAP ISs that receive, process, store, display, or transmit SAP information must operate in compliance with the ATO issued by the AO, which must comply with this issuance, DoDI 8510.01, the DoD JSIG or its successor, and CNSS Instruction 1253, and after consultation with the DCIO for SAP IT for cybersecurity matters. Copies of ATOs will be provided to the DCIO for SAP IT oversight.

b. By complying with this issuance, Annex B of CNSS Policy No. 22, CNSS Instruction 1253, the DoD JSIG or its successor, DoDD 5205.07, and DoDI 5205.11, DoD SAP implementation of the Risk Management Framework and National Security Memorandum 8 requirements is aligned with Intelligence Community Directive (ICD) 503.

c. Additional or compensatory technical and non-technical countermeasures may be included in a system security plan or memorandum for the record issued by the CA SAPCO, after consultation with the Director of the CA SAPCO or designee, be imposed in the interest of safeguarding SAP-protected information in coordination with the CA SAPCO security director and in consultation with the DCIO for SAP IT. These details must be additionally authorized in the ATO issued by the AO.

d. When serving as the National Manager for NSSs, the Director, National Security Agency, pursuant National Security Directive 42 and National Security Memorandum-8, or any Presidential directive or successor order, provides policies and standards for SAP IT systems. Such programs will comply with the policies and standards in accordance with processes outlined in National Security Memorandum 8.

SECTION 6: SETA

6.1. GENERAL.

GSSOs or CSSOs will ensure that their SETA program meets the specific and unique requirements of this issuance.

a. The SETA program applies to all SAP-accessed individuals.

b. General, non-SAP-specific, or company-wide security briefings may be used to form the basis for or supplement the SAP SETA requirement.

c. Training on the program elements; location of the SCG and addendum(s); trends and/or lessons learned from enterprise; program and/or location specific security incidents; and SAPF location-specific parameters is required and will supplement any standardized non-specific training used. Program elements will be identified by the cognizant government office.

d. For an umbrella, oversight level, or portfolio, specific program elements may be developed by cognizant CA SAPCO to minimize the burden of briefing each SAP contained within.

e. If there is a campus, base, or enterprise standardized non-specific SETA training, the CA SAPCO or designee will decide who approves the program.

f. SETA compliance will be annotated in the annual DoD Security Compliance Inspection Checklist and provided to the responsible PSM or PSO in accordance with this issuance.

g. If required or approved by the CA SAPCO or cognizant government agency, a program may have a SETA plan for the entire program. The plan will include items from the PPP and a plan for how the SETA training will be accomplished.

6.2. PSM OR PSO.

PSMs or PSOs will approve the SETA program of assigned SAPs, including the cybersecurity certification requirements in accordance with DoDM 8140.03. This may be a standalone document or incorporated into the SAPF's SOP. To the greatest extent possible, the SOP should be unclassified or collateral classified.

6.3. GSSO AND CSSO.

GSSO(s) and CSSO(s) will:

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

b. Annotate compliance with SETA requirements in the DoD Security Compliance Inspection Checklist and provide to the responsible PSM or PSO in accordance with this issuance.

6.4. INITIAL AND ANNUAL TRAINING.

a. All personnel with SAP access require initial training before or during the briefing to their first DoD SAP and must receive annual training thereafter to acknowledge their responsibilities while accessed to one or more SAPs. At a minimum the training must be updated when:

(1) There are changes in the SAP SCG relevant to the program.

(2) There are changes to information within the SCG annex that is, or no longer is, protected by the SAP.

(3) There are any changes to the acknowledged or unacknowledged status of the SAP.

(4) There are other major changes within, or threats to, the program as determined by the PSM or PSO.

b. Initial and annual (once every 365 days) training by the PSM or the PSO, the GSSO or CSSO, as applicable, or designee may take several different forms including, but not limited to:

(1) Face-to-face briefings, which is the preferred method.

(2) Computer-based presentations sent via e-mail on the appropriate classified network.

(3) Single page data sheets requiring individual review and signature.

(4) Other PSM- or PSO-approved methods, which must be included in or added to the SOP.

c. Individuals who are accessed at an umbrella or oversight level may be pointed to locations where CPI may be reviewed, rather than reviewing CPI for each annex.

d. SAP-accessed individuals will be briefed by the appropriate SAP security personnel (e.g., PSMs, PSOs, GSSOs, and CSSOs) on individual reporting requirements during initial briefings and during annual training in accordance with this issuance.

e. Training will be recorded by using the SAP training record template developed and provided by the CA SAPCO and uploaded in the authoritative source upon completion.

f. CA SAPCOs may require supplemental, situational, or event-driven training.

SECTION 7: SECURITY INCIDENTS, INQUIRIES, AND RECONSIDERATIONS

7.1. SECURITY INCIDENTS.

a. Security incidents must be investigated, and actions must be taken to safeguard classified national security information (including SAP), ensure that the adverse effects of loss or compromise of classified information are mitigated, and promote individual and collective accountability through the application of appropriate corrective actions.

(1) Security incidents involving classified information will be handled by trained SAP professionals and investigated in accordance with this issuance and Volume 3 of DoDM 5200.01 or successor policy and additionally for contractors, in accordance with Part 117 of Title 32, Code of Federal Regulations (CFR).

(2) All actual or potential security incidents will be reported in accordance with the procedures in this issuance through organizational leadership to the PSM or the PSO immediately, to the extent possible, and no later than 24 hours after discovery.

(a) The appointed inquiry officer will conduct an initial inquiry to determine the scope of the incident and include their inquiry with the initial report made to the PSO.

(b) If the PSO concurs with the initial inquiry, incidents deemed security infractions will be maintained locally by the GSSO or the CSSO and reviewed during compliance inspections. The PSO will manage incidents initially categorized as violations in accordance with this section.

(c) Insider threat related information that includes damage to the United States as a result of espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of department resources or capabilities will be reported to DoD Component insider threat programs in accordance with DoDI 5205.16. The CA SAPCO may establish concurrent reporting requirements to the PSO or another designee. The servicing MDCO and defense criminal investigation organization will be notified as appropriate and in accordance with DoDI 5205.16.

(3) A security inquiry in response to infractions or violations involving SAP information and SAP-accessed personnel will be conducted in accordance with Paragraph 4.1.g of this issuance. All security incidents categorized as violations will be coordinated through the organizational leadership to the PSO or PSM for closure and additional action(s).

(4) The PSM or the PSO will notify the GAM of any security incident involving CPI related to a SAP contract.

(5) The PSM or the PSO will provide the details of inadvertent security infractions and security violations to the cognizant CI authority to assess potential insider threat or foreign intelligence nexus.

(6) The CA SAPCO or designated security director will review all security incident reports submitted by the inquiry official.

(7) The CA SAPCO or designated security director will notify the DoD SAPCO and other CA SAPCOs of actual or potential security incidents impacting SAPs with multiple cognizant security authorities.

b. The following will be reported to the CA SAPCO and the DoD SAPCO, which will report to the DepSecDef and the USD(I&S):

(1) Actual or potential compromises involving DoD SAPs.

(2) Results of the compromise or inquiries.

(3) Weaknesses or vulnerabilities in existing SAP policy or procedures that contributed to an actual or potential compromise.

(4) A determination if there was a serious security incident in accordance with DoDD 5210.50.

c. Personnel determined to have had unauthorized or inadvertent access to SAP information will be interviewed by the GSSO or CSSO, as applicable, and the PSO or the PSM to determine the extent of the exposure, unless otherwise directed by the PSO. Personnel will complete inadvertent disclosure statements, as appropriate.

(1) Personnel with eligibility for access to classified information who signed a Standard Form 312, "Classified Information Nondisclosure Agreement," (available at https://www.gsa.gov/forms) and have a lifelong obligation to protect classified information must sign an inadvertent disclosure statement.

(2) Personnel without eligibility for access to classified national security information may be requested to complete an inadvertent disclosure statement.

(3) Any refusal to sign an inadvertent disclosure statement by personnel inadvertently exposed to SAP information will be reported by the GSSO or the CSSO through organizational leadership and to the PSM or PSO immediately, to the extent possible, and no later than 24 hours.

(4) Security 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, the CSSO, the PSO, and/or the PSM to determine the extent of the exposure and determine any intent to disclose body camera footage. These personnel may be asked to sign an inadvertent disclosure agreement. The PSO will review any body camera recordings in secure spaces and refer any potential disclosures to servicing legal counsel. The CA SAPCO will determine if a damage assessment is necessary.

d. The PSM or the PSO, in coordination with the GAM, will notify the OCA responsible for classification of the information associated to the security violations, and may request a damage

assessment to determine the risk to national security for significant security incidents involving SAPs from an actual or potential compromise.

(1) The damage assessment will be conducted and completed in accordance with Volume 3 of DoDM 5200.01 or successor policy.

(2) The damage assessment results will be reported to the OCA, the CA SAPCO, and the DoD SAPCO, who will notify the Director of Security Policy and Oversight, OUSD(I&S).

(3) Upon review of the assessment, the OCA may direct changes in information classification or handling. Downgrading of the classification for SAP information must be coordinated through the CA SAPCO and DoD SAPCO for SecDef or DepSecDef approval.

e. CA SAPCO security directors will ensure contracts include requirements for companies to cooperate with preliminary inquiries and all other relevant fact-finding by the government related to SAP-accessed personnel and company practices while supporting DoD SAP requirements.

7.2. SECURITY INQUIRIES.

A security inquiry will be conducted for all security incidents involving SAP information or SAP-accessed personnel.

a. Security Inquiry and Scope.

(1) PSMs or PSOs will determine the scope of the inquiry and appoint an inquiry official in writing. Based on the inquiry's findings, PSMs or PSOs will determine if an additional security investigation of the incident is required in accordance with Volume 3 of DoDM 5200.01 or successor policy.

(2) The security inquiry will:

(a) Characterize the incident and determine whether the security incident is an infraction or a violation.

(b) Determine the facts and circumstances of the incident including. but not limited to:

1. When, where, and how the incident occurred.

2. The persons, situations, or conditions that caused or contributed to the incident.

3. If SAP information was compromised.

4. If the classification level of the SAP information was disclosed.

5. The specific classified information or material involved.

6. If the information was properly and currently classified.

7. If the information was officially released before the incident.

8. If an IS is involved or affected.

(c) Document the steps taken to locate and recover the material if classified material is alleged to have been compromised or lost.

(d) Assess the potential damage to national security caused by the incident.

(e) Assess the likely cause, if the incident is substantiated.

b. Initial PSM or PSO Recommendation.

GSSOs will make an initial recommendation for corrective action based on the severity of the incident, to safeguard SAP information and correct or eliminate the conditions that caused or brought about the security incident. Concurrence by the PSM or the PSO is recommended. They will:

(1) Recommend one of the following administrative corrective actions:

(a) No Action.

Retain SAP access with eligibility for additional SAP access.

(b) No Action with Condition.

Retain SAP access with eligibility for additional SAP access pending the completion of a follow-on actions, such as remedial SETA training or SOP updates.

(c) Limit.

Retain current SAP access and temporarily lose eligibility for additional SAP access for a duration determined by the CA SAPCO.

(d) Suspend.

Temporarily lose eligibility for current SAP access and additional SAP access, consistent with Paragraph 9.4. of DoDM 5200.02.

(2) Submit the initial security inquiry report and initial recommendation for corrective action to the CA SAPCO, in coordination with the organization's chain of command, through the PSM or SPO, no later than 10 business days after receiving notification of a security incident.

c. Initial CA SAPCO Corrective Action Determination.

The CA SAPCO or designated security director will make an initial corrective action determination for all security inquiries, based on the severity of the incident, totality of

circumstances, and to correct or eliminate the conditions that caused or brought about the security incident. They will:

(1) Make one of the initial administrative corrective actions recommended by the PSM or PSO in Paragraph 7.2.b.

(2) Notify the recommending PSM or PSO of the initial corrective action determination no later than 7 business days after receiving a security inquiry report.

(3) Notify DoD SAPCO, other stakeholder CA SAPCOs, and the recommending PSM or PSO's chain of command of any "Limit" or "Suspend" initial administrative corrective actions.

(4) Ensure all security incidents and associated corrective actions are appropriately documented in both JADE and the DISS, as well as any successor systems to those databases.

d. Initial Determination Notification and Reporting.

PSMs or PSOs:

(1) In coordination with the GAM or the CAM, the GSSO or the CSSO, the commander, or appropriate industry official, will notify the subject(s) of the security incident of the initial determination associated to the security inquiry.

(2) Must ensure all security incidents involving personnel with access to SCI are reported to the servicing special security officer (SSO).

e. Final PSM or PSO Report and Recommendation.

PSMs or PSOs will submit the final security inquiry report and recommendation for corrective action to the CA SAPCO, in coordination with the organization's chain of command, no later than 30 business days after receiving notification of a security incident. Final security inquiry reports that require more than 30 business days to complete must have an approved extension memorandum from the CA SAPCO or designated security director. PSMs or PSOs will:

(1) Make a final recommendation for corrective action based on the severity of the incident, to safeguard SAP information and correct or eliminate the conditions that caused or brought about the security incident.

(2) Recommend one of the following administrative corrective actions:

(a) Reinstate.

Remove "Limit" or "Suspend" status and retain eligibility for current or additional SAP access.

(b) Suspend.

Temporarily lose eligibility for current SAP access and additional SAP access.

(c) Debrief for Cause.

Debriefed from current access, and ineligible for SAP access.

(d) Revoke.

Permanently ineligible for SAP access.

f. Final CA SAPCO Determination.

The CA SAPCO or designated security director will make a final corrective action determination for all security inquiries, based on the severity of the incident, totality of circumstances, and to correct or eliminate the conditions that caused or brought about the security incident. They will:

(1) Apply one of the following final administrative corrective actions:

(a) Reinstate.

Remove "Limit" or "Suspend" status and retain eligibility for current or additional SAP access.

(b) Suspend.

Temporarily lose eligibility for current SAP access and additional SAP access.

(c) Debrief for Cause.

Debriefed from current access, and ineligible for SAP access.

(d) Revoke.

Permanently ineligible for SAP access.

(2) Notify the recommending organization and PSM or PSO of the final corrective action determination no later than 14 business days after receiving a final security inquiry report.

(3) Notify DoD SAPCO and other stakeholder CA SAPCOs and the organization and PSM or PSO's chain of command of the final corrective action.

(4) Ensure all security incidents and associated final corrective actions are appropriately documented in both JADE and DISS, as well as any successor systems to those databases.

(5) Retain final security inquiry reports as required for effective and efficient operation of the organization, or as law or regulation requires.

g. Final Determination Notification and Reporting.

PSMs or PSOs:

(1) Will notify the subject(s) of the security incident of the final determination associated with the security inquiry, in coordination with government personnel, the GAM, the GSSO, the commander, general counsel, and human resource personnel, or, for contractor personnel, the CAM, the CSSO, or other appropriate industry official, and the GCA.

(2) Must ensure all security incidents and final corrective actions involving personnel with access to SCI are reported to the servicing SSO.

7.3. RECONSIDERATIONS.

a. All persons who receive an administrative corrective action that results in a determination impacting their access to DoD SAPs may request reconsideration of the decision.

b. CA SAPCOs or security director, will provide an administrative reconsideration process, to include:

(1) Provision of a comprehensive written explanation of the basis for the denial or revocation.

(2) Provision of any documents, records, and reports upon which a denial or revocation is based and to the extent they would be provided if requested under applicable law, to include the Freedom of Information Act or Section 552a of Title 5, U.S.C. (also known and referred to in this issuance as the "Privacy Act").

(3) An opportunity to respond, in writing, following the receipt of relevant documentation, to request a review of the determination.

(4) An opportunity to request review by the CA, or their designee, who may either make a final determination themself or return the requester's package to the CA SAPCO for additional fact-finding.

c. If the CA, or their designee, personally certifies on a case-by-case basis that a procedure set forth herein cannot be made available without extraordinarily damaging national security interests, reconsideration will not be made available for the particular individual. This certification will be conclusive. Should it be determined on a case-by-case basis that the right to reconsideration procedures cannot be invoked in a manner that is consistent with the national security, the individual may be denied CA, or their designee, review.

d. The reconsideration process will be available to all individuals, regardless of affiliation (military, civil service, or contractor) who have access to DoD SAPs.

e. AAA disapprovals of nominations based on insufficient NTK are final. The original requester may submit to the original AAA additional justifications to establish sufficient NTK.

f. The reconsideration process does not create or confer on any person any right to a judicial review of these procedures, their implementation, or decisions or actions rendered there under. Nor does it create or confer any right, benefit, or privilege, whether substantive or procedural, for

access to classified national intelligence or create or confer any substantive or procedural right, benefit, or privilege enforceable by any party against the United States or any agency, department, or instrumentality of the executive branch, its officers or employees, for any other person.

SECTION 8: SAP SECURITY COMPLIANCE INSPECTIONS

8.1. GENERAL.

The SAP security compliance process represents a unified and streamlined approach to the SAP security compliance inspections.

a. All organizations supporting SAPs are subject to the security compliance inspection process. No organization is exempt from compliance inspections.

b. The detailed guidance, procedures, and security inspection checklist for conducting security compliance inspections are posted on the DCSA website at https://www.dcsa.mil/Industrial-Security/Special-Access-Programs-Templates/.

c. Inspections require submission of 60-day corrective action plans by the inspected activity within 30 days of receiving the final report.

d. CA SAPCOs or their designees will assign inspection teams appropriately scoped with the right skill sets and number of personnel required to conduct the inspection.

e. Prime contractors must be present at all inspections of their subcontractors.

8.2. EXTERNAL INSPECTIONS.

CA SAPCO-appointed inspectors will conduct inspections to validate that SAP security processes and procedures comply with applicable DoD policies and implemented in this issuance and ensure that any risks of SAP information being compromised are both understood and managed. External inspections will be executed with the least amount of impact to the SAP, while maintaining a proficient, equitable, and comprehensive review. The four external inspections are core compliance inspections; general inspections; re-inspections; and unannounced or no notice inspections.

a. Core Compliance Inspections.

(1) Core compliance inspections will be conducted at the direction of the CA SAPCO, PSM, or PSO, or at the request of the inspected activity at a minimum of every 2 years. The core compliance inspection addresses DoD or CA SAPCO SEIs and the core functional areas (CFAs):

(a) Security management.

(b) Personnel vetting.

(c) Accountability.

(d) Physical security.

(e) Cybersecurity.

(f) Security education.

(2) In addition to CFAs, these inspections must include a review of DoD SAPCO-issued SEIs.

b. General Inspections.

General inspections require a complete and thorough validation of all functional areas.

(1) CA SAPCOs may direct general inspections at their discretion but will direct them upon an unsatisfactory rating.

(2) Overall unsatisfactory ratings result from circumstances and conditions indicating the program management personnel within a SAPF have lost, or are in danger of losing, the ability to adequately safeguard the classified material for which they are accountable.

c. Re-inspections.

(1) Re-inspections are required when:

(a) A core compliance or general inspection results in an unsatisfactory rating in one or more functional areas but does not result in an overall unsatisfactory rating.

(b) Deficiencies in one or more CFAs or SEIs result in an unsatisfactory rating for each specific CFA or SEI.

(2) Re-inspections must be conducted no later than 90 days from the issuance of the final inspection report and focus on CFA or SEI areas that resulted in unsatisfactory ratings.

d. Unannounced or No Notice Inspections.

Unannounced or no notice inspections can be general inspections or core compliance inspections conducted without notice and at the discretion of the CA SAPCO or designee.

(1) A security representative from the prime contractor must be present and participate during inspections of subcontractors.

(2) Designated personnel will serve as inspection team chiefs, assign ratings, conduct in- or out-briefings, and be responsible for completing the security inspection report.

8.3. EXTERNAL INSPECTION COORDINATION AND REPORTING.

a. All inspections will be coordinated among the stakeholder SAPCOs and conducted jointly to the greatest extent possible. Stakeholder SAPCOs, regardless of being present for the inspection, agree to accept joint inspection results when sharing a SAPF to minimize or eliminate the impact of multiple inspections on units.

b. Core compliance inspections involving multiple SAP organizations will be fully coordinated between participating DoD organizations by the assigned team chiefs.

c. Each organization is responsible for publishing its report. Critical findings will be shared so that the community applies a standardized approach to compliance.

8.4. INTERNAL OR SELF INSPECTIONS.

GSSOs or CSSOs conduct, at a minimum, annual internal or "self-inspection" for all SAPFs for which they are assigned responsibility. Inspectors will use the security compliance inspection template referenced in Paragraph 8.1.b. and document any deficiencies in a corrective action plan. The corrective action plan will detail planned actions to correct deficiencies in areas deemed unsatisfactory. All supporting information will be included in the self-inspection report.

a. The documented results of self-inspections will be retained until the next external inspection is completed. All outstanding items must be completed before the destruction of any compliance documentation in accordance with the approved records schedule.

b. Self-inspection review reports must be signed by the GAM and organization commander for governmental locations, or by the CAM for industry locations. The report will also include a 60-day corrective action plan. The plan will ensure that the GAM and commander or CAM, as applicable, are aware of the operations status of SAPs for which they have oversight and management.

c. The documented results of the self-inspections will be submitted to the PSM or PSO for coordination within 30 days of completion. For self-inspections that result in the need for corrective action, updates must be provided every 30 days thereafter until complete. The PSM or PSO will be notified immediately if the self-inspection discloses the loss, compromise, or suspected compromise of SAP information. Security incident reporting will be in accordance with Section 7 of this issuance.

d. In addition to all CFAs, inspectors will be required to validate SEIs. The CA SAPCO will provide input on the trends and provide recommended SEIs to the DoD SAPCO.

8.5. STAFF ASSISTANCE VISIT (SAV).

PSMs or PSOs will conduct SAVs at their discretion, if a risk of SAP exposure is apparent based on security practices, or as directed by the CA SAPCO or requested by an organization. During a SAV, the PSM or the PSO or the designee will review security documentation and provide assistance or direction as necessary.

a. SAVs may include, but are not limited to, review of:

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

(2) Outstanding government action items.

(3) Administrative security documentation (e.g., SOP, CSSO, and information assurance 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 PSM or the PSO will provide a SAV report to the organizational leadership and GSSO or CSSO detailing the scope of the SAV and identifying all observations and findings requiring resolution before the next security compliance inspection.

(1) A copy will also be provided to the SAP IS AO(s), CA SAPCO, and any other applicable parties for any observations relating to systems accredited to process SAP, who will then coordinate with the DCIO for SAP IT.

(2) During the SAV, the PSM or the PSO will pass concerns that require follow-up before the next inspection to the GSSO or the CSSO.

(3) The PSM or the PSO will provide guidance and direction to assist the organization in the development of an effective and standardized security program.

c. A compliance inspection may not be converted to or reframed as a SAV to prevent the formal documentation of unsatisfactory findings.

8.6. DEFICIENCIES.

After an external inspection is completed, the PSM or the PSO will determine the rating of the inspection based on the quantity and quality of deficiencies identified and the risk of a compromise to classified information. Deficiencies will be defined as a finding or deviation from policy.

8.7. RATINGS.

External inspection ratings are COMMENDABLE, SATISFACTORY, MARGINAL, and UNSATISFACTORY.

a. If the inspection reveals no deficiencies, the result is a COMMENDABLE rating.

b. If the inspection confirms the effective implementation of security requirements and the absence of any serious security issues, the result is a SATISFACTORY rating.

(1) Discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days.

(2) Place the organization on an inspection cycle not to exceed 24 months.

c. If the inspection reveals deficiencies that could compromise classified information if left uncorrected, the result is a MARGINAL rating. If the rating is MARGINAL, the inspector will:

(1) Discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days.

(2) Schedule a re-inspection on the marginal areas within 90 days of the command receiving the final inspection report. The inspecting organization may make the determination if an in-person re-inspection is required.

d. If an inspection reveals deficiencies that would likely lead to or have already resulted in the loss or compromise of classified information, the result is an UNSATISFACTORY rating.

(1) The CA SAPCO will be notified immediately of inspections or re-inspections resulting in an UNSATISFACTORY rating.

(a) If a facility receives an UNSATISFACTORY rating, either as an overall inspection rating, in a CFA, or a DoD SAPCO SEI, this will result in an immediate shutdown of operations in that functional area(s) until the identified security concerns are remediated.

(b) Any requests for continued operations following an UNSATISFACTORY rating will be submitted to the CA SAPCO via the PSM or PSO.

(2) If the rating is UNSATISFACTORY, the inspector will:

(a) Discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report no later than 30 days.

(b) Schedule a compliance security review to be conducted within 90 days.

e. The inspector must conduct due diligence before the inspection to address areas of major vulnerabilities based on the facility's location and unique program risk.

SECTION 9: VISIT PROCEDURES

9.1. GENERAL.

For all visits, JADE or its successor will be used for access verifications as long as the visited location has the ability to verify program access for the visiting personnel. If the visited location cannot verify program accesses in JADE or its successor, a written or electronic visit notification must be sent before the visit, containing the person's name, clearance level, program access to be discussed, point of contact, date of visit, and purpose. All requests may not exceed 12 months unless approved by the PSO.

a. Industry to Industry.

Approval by the appropriate GAM or designated representative is required for all visits to SAPFs or participation in SAP activities associated with a government contract.

(1) Visits between the sites of a prime contractor and the prime's subcontractors will be approved by the CAM or their designee.

(2) A written or electronic visit notification must be approved before visiting a SAPF, and industry centralized personnel vetting databases may be used for access verification if authorized in writing by the responsible PSM or PSO or CA SAPCO.

b. Industry to Government.

Approval by the appropriate GAM or designated representative is required for all visits to SAPFs or participation in SAP activities.

c. Government to Government.

A visit to a government location is coordinated through a government office using JADE or successor system as the official database of record and does not require a formal visit request.

d. Government to Industry.

A visit to an industry location is coordinated through the GCA or other government office to the appropriate industry representative using JADE, or any successor system, as the official database of record. A government visit to industry to conduct security oversight does not require a formal visit request.

9.2. ADVANCE NOTICE.

SAP-accessed personnel must make every effort to provide advance notification of the visit to their GSSO or CSSO. Visitors who intend to courier SAP material must comply with Paragraph 4.5.c.

9.3. UNANNOUNCED AND NON-VALIDATED ARRIVALS.

Access may be denied if a visitor arrives at a government or contractor SAPF without the ability to validate requisite SAP accesses. PSMs or PSOs and supporting security staff members, as designated by the PSM or the PSO, may visit all SAPFs under their responsibility without first giving notice.

9.4. VISITOR IDENTIFICATION VALIDATION.

The positive identification of each visitor will be made using an authorized credential in accordance with Volume 3 of DoDM 5200.08. The credential's identification number will be annotated on the visit request. For positive identification in locations associated with a DoD SAP, USG personnel should consider the implications of the use of identification that could reveal their association with the USG or with a specific agency or component.

9.5. VISITOR ESCORT.

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 without SAP access visiting a SAPF must be approved in advance by the CA SAPCO or designee. Foreign nationals with current SAP access must meet all other visit requirements in this section as well as all other foreign visit requirements, but do not require re-vetting for official visits.

c. The PSM or the PSO or the designee will determine whether an internal warning system, such as rotating light beacons, is necessary to warn accessed occupants of the presence of non-accessed personnel or personnel without all the required SAP accesses for that space.

(1) The PSM or the PSO or the 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.

(2) The other or additional methods will be included in the SAPF SOP.

9.6. VISIT REQUEST TERMINATION OR CANCELLATION.

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.

9.7. VISITOR RECORDS.

a. Unless a PSM- or PSO-approved electronic visitor record is on file, the visitor record will contain the visitor's:

(1) First and last name.

(2) Organization or affiliation ("Self" is not an acceptable input).

(3) Date visited.

(4). Time in and out.

(5) Sponsor.

(6) Citizenship.

(7) Purpose.

b. Visitor logs will be retained for 1 year from the date of the last entry in accordance with Paragraph 3.14.

9.8. CONGRESSIONAL VISITS.

a. All communications and information regarding DoD SAP with congressional members or their staff will be coordinated through the DoD SAPCO and the CA SAPCO.

b. In the event of the unannounced arrival of a congressional delegation, DoD and industry employees accessed to DoD SAPs will contact the GAM or the CAM, as applicable, for coordination with the PSM or the PSO for guidance. The PSM or the PSO will notify the CA SAPCO and receive guidance regarding the appropriate SAP access to support the congressional delegation.

SECTION 10: CONTRACTING

10.1. GENERAL.

The GCA awards contracts on behalf of the government and coordinates security requirements with the PSM or the PSO. In accordance with Subpart 4.4. of the Federal Acquisition Regulation and Volume 1 of DoDM 5220.32, the contracting officer's representative or designee initiates the DD Form 254 and forwards it to the PSM or the PSO to prepare and submit to the NISP Contract Classification System (NCCS) for processing. The GCA, contracting officer's representative, and security officer sign the DD Form 254 for each prime contract, which shall be incorporated into the contract as a material term or condition. For subcontracts, the prime CSSO or designee prepares a DD Form 254 and forwards it to the PSM or the PSO for review before release to subcontractors via the NCCS. All documents associated with the contract (e.g., statement of work, performance work statement, or statement of objectives) must be safeguarded in accordance with the applicable SCG. The GCA is responsible for oversight of contract performance and ensuring compliance with all applicable procurement laws, regulations, and policies. Relevant government oversight personnel shall ensure the GCA is notified of any contract administration or performance issues in a timely fashion.

a. The DD Form 254 must be completed in accordance with the standards and strictures outlined in the instructions for completing DD Form 254 and should not include lengthy attachments that merely repeat information, policy, and procedures contained in any other security policies, which should instead be incorporated by reference. The DD Form 254 contains:

(1) An addendum that contains security guidelines and any HVSACO, collateral, or SAP-level information.

(2) Any collateral and SCI requirements, including disposition of information, material, and facilities.

(3) A listing of all security policy and procedural references applicable to the execution of the contract, such as this issuance.

(4) Explicit security guidance for contract execution.

b. The PSM or the PSO will notify the CA SAPCO if a prime contractor imposes any security requirements exceeding those provided for in this issuance on a sub-contractor. The PSM or the PSO will notify the GCA, who will generate a memorandum for signature by the CAM addressing the issues to the CA SAPCO, along with the proposed corrective actions.

c. To the greatest extent possible, DD Forms 254 for SAP contracts will be unclassified or CUI and processed via the NCCS. Unclassified and CUI DD Form 254s may be supplemented by a separate, classified SAP addendum.

(1) SAP addendums will list specific SAP security information, to include the period of performance and specific PIDs associated to the contract issued by the GCA.

(2) Contractors will not be allowed access to SAPs, whether by individual PID or by portfolio, that are not identified on the SAP addendum.

(3) SAP portfolios may be included on addendums.

d. Subcontractor DD Form 254s must be signed by the subcontractor.

e. Contractor materials may be stored at a government location upon closing of a SAPF, contract, or program.

10.2. CLEARANCE STATUS OF CONTRACTORS.

All prime contractors and sub-contractors who require access to SAPs must be cleared pursuant to Part 117 of Title 32, CFR.

10.3. SECURITY AGREEMENTS AND BRIEFINGS.

a. A prime contractor is responsible for issuing subcontracts and entering into a formal relationship with prospective subcontractors.

(1) The prime contractor will obtain approval from the PSM or the PSO before any release of SAP information.

(2) When conducting business with non-SAP briefed subcontractors, prime contractors will ensure SAP information is not inadvertently released.

(3) Any relationship with a prospective subcontractor for SAP-related or security-related services or items requires coordination with the GCA, and security review and concurrence by the PSM or PSO.

b. Before the release of any SAP information, the prime contractor must brief any prospective subcontractor regarding the procurement's enhanced special security requirements.

(1) The prime contractor will pre-coordinate arrangements for subcontractor SAP access with the PSM or the PSO.

(2) The CSSO will complete a subcontractor or supplier data sheet for submission to the PSM or 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.

(3) The CSSO will include the reason for considering a subcontractor and attach a proposed DD Form 254 to the subcontractor or supplier data sheet.

(4) The DD Form 254 will be tailored to be consistent with the proposed support being sought and be classified based on its content.

10.4. INDEPENDENT RESEARCH AND DEVELOPMENT (IR&D).

a. The use of SAP information for a contractor IR&D effort will occur only with the specific written permission of the GCA and the GAM.

(1) A document establishing a government–contractor relationship, such as a letter defining the authority to conduct IR&D, or a bailment agreement, will be created so that a DD Form 254 can be applied. The IR&D DD Form 254 will be processed in the same manner as traditional DD Form 254s, as described in Paragraph 10.1.

(2) The procedures and requirements necessary for safeguarding SAP information will be outlined in the IR&D DD Form 254.

(3) The IR&D establishing document, DD Form 254, and appropriate classification guidance will be provided to the contractor.

b. Subcontracting of IR&D efforts with SAP information will follow the same process as outlined in Paragraph 10.4.a.

c. IR&D operations and documentation containing SAP information are subject to security oversight and inspection in the same manner as other SAP information in the possession of the contractor under contract.

10.5. DISPOSITION AND CLOSE-OUT ACTIONS.

a. Contract close out will be handled in accordance with governing law and regulation and as supplemented by the requirements of this section.

b. The CSSO or their designee will inventory, dispose of, request retention, or return for disposition all SAP material at contract completion or close-out or at the completion or close out of a government-contractor IR&D relationship.

(1) Request for proposals, solicitations, or bids and proposals contained in SAP files will be reviewed and screened by CSSOs in accordance with DoD Component records disposition instructions.

(2) Disposition of information by document control number, or if there is not a document control number by title and date, will be submitted to the PSM or PSO and GCA for concurrence.

(3) Upon contract close-out, requests for retention of classified information will be submitted to the GCA and GAM through the PSM or PSO for review and approval.

(4) The contractor will not retain any SAP information unless specifically authorized in writing by the GCA.

(5) A final DD Form 254 will be issued for the continuation of SAP security requirements. The PSM or PSO will approve storage and control requirements.

c. At the initiation of a closeout, termination, or completion of a contract, the CSSO will develop a termination plan for PSM or PSO approval.

(1) The plan will outline the actions necessary for disposition of residual hardware, software, documentation, SAPF, and personnel accesses documented in a termination plan.

(2) The master classified material accountability record (e.g., log or register) will be transferred to the PSM or the PSO at SAP closeout.

(3) All closeout actions require final approval from the GCA and the PSM or the PSO.

SECTION 11: SAP TECHNOLOGY TRANSFER

11.1. TECHNOLOGY TRANSFER.

a. In addition to the procedures established in DoDI 5535.08, two primary issues must be addressed with all SAP technology transfers.

(1) The first issue is to ensure all technology to be transferred is reviewed to determine if there are any IP restrictions associated with the technology proposed for transfer. If so, those specific items must be clearly annotated with the appropriate restrictive markings.

(2) The second is to ensure that the scope of the gaining SAP SCG is sufficient to protect technology and IP that are to be transferred. If not, the gaining SAP SCG must be updated, and the update approved before transfer.

b. The technology transfer agreement is used to document transfers of SAP technology between DoD and non-DoD Federal Departments and Agencies.

(1) GAMs from both SAPs (losing and gaining) may approve technology transfers that do not involve different categories or level of classification. Additionally, the technology transfer must be coordinated with the gaining PSO. Both GAMs must maintain records of all technology transfers.

(2) Only the CA SAPCO, or authorized designee, may approve SAP technology transfer agreements if the gaining SAP is a different category or classification level than the losing SAP (i.e., unacknowledged to acknowledged).

(3) Transfers of SAP technology to a foreign government will be conducted in accordance with foreign disclosure procedures in DoDIs 2040.02 and 5205.11.

c. CA SAPCO will provide a copy of domestic technology transfer agreements to the Office of the Under Secretary of Defense for Research and Engineering SAPCO pursuant to DoDD 5137.02.

d. Transfer of accountable items will be reflected in the approved accountable property system of record.

11.2. SYSTEM OR CAPABILITY TRANSFERS.

a. A system or capability transfer MOA will be prepared by the GAM, the GSSO, and the PSM or the PSO for any system or capability transferred to or from a DoD Component from a non-DoD organization when the system or capability to be transferred requires continued resources to sustain it.

b. The system or capability transfer MOA must be approved by the CA SAPCO. The system or capability transfer MOA must include:

(1) Description of technology to be transferred (e.g., data, knowledge, equipment).

(2) Gaining and losing organizations.

(3) Roles and responsibilities.

(4) Gaining security office and its contact information.

(5) Personnel vetting access requirements, if beyond standard requirements.

(6) Logistics and sustainment requirements.

(7) IS requirements.

(8) Marking guidelines and instructions.

(9) Contracting review.

(10) Legal review.

(11) Resources necessary to sustain the SAP.

SECTION 12: PERSONNEL VETTING INFORMATION

12.1. INTRODUCTION.

a. All requests for SAP access must be processed in accordance with this issuance.

b. Nominated individuals must meet the requirements of Section 13.

c. AAAs may disapprove the nomination based upon the individual's failure to possess the access eligibility requirements, NTK, or based on unique risk assessment to the program. AAAs will clearly articulate in the remarks on the PAR why they are disapproving the access. Further guidance on disapprovals can be found in Paragraph 13.6. of this issuance.

d. Acceptable types of background investigation for SAP access:

(1) A SAP that protects information up to SECRET requires a minimum of a final SECRET eligibility determination based upon either a Moderate Tier, Tier 3, National Agency Check with Law and Credit, or an Access National Agency Check and Inquiries or equivalent-level background investigation.

(2) A SAP that protects classified information up to TS requires a minimum of a final TS eligibility determination based on a High Tier, Tier 5, single scope background investigation and periodic reinvestigation, or a phased periodic reinvestigation or equivalent-level background investigation.

e. Nominees satisfy SAP eligibility requirements if they have the appropriate clearance eligibility and are enrolled in either a DoD compliant continuous vetting (CV) program (regardless of recorded CE date) that is validated in the DISS or a successor system, or in the ODNI continuous evaluation (CE) system validated in Scattered Castles or a successor system. CV enrollment will be accepted if an individual is not enrolled in a CV program or CE system, a LOCN is required (see Glossary definition).

f. Potentially disqualifying information not previously reported will be assessed by the PSO or the PSM, as appropriate.

g. Additional justification will be required for nominees who do not meet one of the criteria defined in Paragraphs 12.1.g.(1) through 12.1.g.(3). To mitigate this, information is required to be submitted within the remarks section of the PAR to articulate the reason clearly and concisely for the issue, the mitigating factors, and the path forward to resolution. These criteria include:

(1) The nominee not being enrolled in a CV program or CE system.

(2) For contractor nominees, a lack of a current, valid SAP DD Form 254 in accordance with Section 10 of this issuance.

(3) For consultant nominees, a lack of a current, valid consultant agreement.

h. The CA SAPCO decision is final. If the LOCN request is denied, there is no reconsideration process.

i. Nomination packages and associated personnel vetting databases must be administered and maintained in accordance with DoDI 5400.11 and comply with all records management requirements in DoDI 5015.02.

12.2. SAP RECIPROCITY.

a. Joint force integration SAPs may grant access with reciprocity.

(1) A nominated individual with an existing DoD SAP access will not be denied access eligibility to a DoD SAP, or subsequent SAP, of the same sensitivity level, category, and type, provided they:

(a) Have validated NTK.

(b) Have no new potentially disqualifying information.

(c) Meet nomination requirements for SAP access.

(d) Have all 'NO' responses on a PSQ dated within the past 365 days.

(2) CA SAPCOs may grant reciprocity for a nominated individual based on a favorable clearance eligibility determination from an eligibility-granting organization, access to another SAP(s), and valid NTK, provided the most recent PSQ was completed within 365 days. Copies of all such approvals must be maintained with the individual's record of SAP access and be made readily available for review as necessary. This data will be captured and made a part of the individual's record in JADE, or successor system.

b. Strategic enabler SAPs do not grant access through reciprocity.

12.3. INDOCTRINATION BRIEFINGS.

SAP-indoctrinated personnel that are authorized to conduct indoctrination briefings will ensure individuals sign the SAPIA before indoctrination in accordance with E.O. 12968, acknowledging the requirements for gaining access to SAP(s) and the SAP-specific unique requirements. This requirement is for nominated U.S. citizens only.

a. The indoctrination is a security-focused briefing to educate an individual on what the SAP's CPI and subsequent guidance are and how to properly safeguard them.

b. At a minimum, indoctrination briefings will cover topics approved by the PSO or the PSM and within the SAPF SOPs.

c. SAP indoctrinations will be conducted only after the PAR has been approved and the SAPIA has been signed.

(1) These procedures must also be followed for cleared foreign nationals.

(2) If a suitable indoctrination agreement or non-disclosure agreement does not exist in the foreign partner's language, coordinate with DoD SAPCO at the beginning of the access approval process.

d. Individuals who are accessed at an umbrella or oversight level, or to a portfolio, may be pointed to location where CPI may be reviewed, rather than reviewing CPI for each sub-compartment or annex.

e. PAR and indoctrination agreement requirements can only be waived by the SecDef, the DepSecDef, or the designee.

f. Indoctrinating foreign nationals to SAP should follow guidelines set forth in the security agreement that governs the SAP and the individual's access to U.S. classified information. Generally, the U.S. Program Indoctrination Agreement is not an appropriate form as foreign nationals are not subject to U.S. law.

12.4. POLYGRAPHS.

a. Personnel accessed to DoD SAPs are subject to CI-scope and issue-based polygraphs in accordance with DoDI 5205.11 and DoDI 5210.91.

(1) Any individual with SAP access who refuses a polygraph examination will have their SAP access suspended immediately.

(2) Issue-based polygraph examinations may be used to resolve issues related to SAP access.

(3) CI-scope polygraph examinations must not be used as the only basis for granting or denying access to DoD SAPs.

(4) Exceptions to these stipulations will only be granted by the DepSecDef.

b. The DepSecDef is the approval authority for the use of polygraph examination as a mandatory access determination requirement; the requirement must be consistently applied to all candidates in accordance with DoDI 5210.91. CI Scope polygraph examinations must not be used as the only basis for determining eligibility for access to DoD SAPs.

12.5. BILLET MANAGEMENT.

CA SAPCOs, in coordination with DoD SAPCO, may establish or authorize SAP billet structures or access quotas that assign individual access by organization and duty position to SAPs under their cognizance.

a. Billets for security personnel and other required operational roles supporting ISs (e.g., ISSM, IS security officer) will count against billet structure or access quotas and need to be included in billet structures.

b. Both the security and operational IT roles must be accounted for on the billet request for approval to ensure the billet structure is properly annotated in the system of record.

c. Personnel serving in a SAP in two different employment statuses (e.g., a Military Reserve officer who is also a cleared defense contractor) will encumber a billet for each of their statuses to ensure access is severable and clearly attributable to NTK and eligibility.

12.6. PERSONNEL VETTING FILES.

Records must be maintained within a personnel vetting file for each SAP-accessed individual.

a. JADE, or any successor system, is the database of record for SAP personnel vetting.

b. The personnel vetting file for each SAP-accessed individual will be maintained in JADE, or any successor system, by the responsible SPO, PSM, PSO, GSSO, or CSSO or designee.

c. Cleared defense contractors that do not have access to JADE, or any successor system, must maintain either hard-copy or electronic records (preferred if practical).

d. Personnel vetting files will include, but are not limited to:

(1) PSQs and supplemental information as required by the CA SAPCO.

(2) DD Form 254 or consultant agreements for contractors, as necessary.

(3) PARs.

(4) Continuation of access (COA) approvals.

(5) SAPIAs.

(6) SETA records.

(7) Foreign travel records.

(8) Foreign contacts records, including personal, business, and suspicious contacts.

(9) Inadvertent disclosure records.

(10) Reports of security infractions and violations.

(11) Potentially disqualifying information records.

(12) LOCNs, as necessary.

12.7. CONGRESSIONAL ACCESS REQUIREMENTS.

Guidance on congressional access to DoD SAPs is in DoDI 5205.11.

12.8. INDIVIDUAL REPORTING REQUIREMENTS.

All SAP-accessed personnel will report to the PSM, the PSO, and the GSSO or CSSO, as applicable, any information, in addition to that identified in the PSQ, about themselves or others that may pose an undue risk to the SAP or possibly affect an individual's access to SAP(s).

a. General reporting requirements are found in DoDM 5200.02.

b. Additionally, all DoD personnel with access to at least one SAP must comply with all DoDM 5200.02 reporting requirements, regardless of approved level of eligibility for access to classified national security information and position sensitivity, in accordance with the November 2, 2020 USD(I&S) Memorandum.

(1) DoDM 5200.02 reporting must be provided to the PSM, the PSO, the GSSO or CSSO, as applicable, and the collateral security manager.

(2) Additionally, personnel with access to a DoD SAP that also have access to SCI must provide DoDM 5200.02 reporting to the servicing SSO.

c. Reporting will comply with requirements defined in the November 2, 2020 USD(I&S) Memorandum.

(1) Foreign Travel.

Report all official and unofficial foreign travel in accordance with Section 14 of this issuance.

(2) Security Incidents.

Immediately report all security infractions and violations to the PSM, PSO, and GSSO or CSSO, as applicable, in accordance with this issuance.

(3) Reportable Contacts, Activities, Indicators, and Behaviors.

SAP-accessed personnel will report to the PSM, PSO, and GSSO or CSSO, as applicable, in accordance with Section 4 of DoDD 5240.06.

12.9. GSSO AND CSSO REPORTING REQUIREMENTS.

At a minimum, GSSO and CSSO must report, in writing, to the PSM or PSO:

a. Any notification by a SAP-accessed individual or an individual for whom access has been requested that they no longer wish to perform on the SAP activities.

b. Any individual who refuses to sign a SAPIA. If a SAPIA is not signed, SAP access will not be granted.

c. All changes in the employment status of SAP-accessed personnel.

d. Changes or modifications to SAP area accreditations.

12.10. DEPLOYED OR TEMPORARILY ASSIGNED PERSONNEL.

Personnel assigned away from their home location for over 180 days will be debriefed unless they have a continued NTK at their deployment location.

a. Exceptions to this requirement must be approved in writing by the CA SAPCO.

b. This debrief approach will apply to similar unbroken absences including, but not limited to, a leave of absence due to medical, parental leave, and National Guard or military activation.

12.11. COA.

COA is negotiated between the losing and gaining organization. Approval must be maintained in the personnel database of record (i.e., JADE or any successor) and there must be a signed SAPIA on record. Individuals with SAP access may request COA under the following guidelines:

a. The individual's personnel vetting investigation must be at the appropriate level and the individual must be enrolled in the CV program. The individual must also provide an updated PSQ.

b. For contractors, individuals must support the same contract to transfer SAP access.

c. No previously unreported potentially disqualifying information exists that could affect the individual's continued eligibility for access to SAP(s). The AAA and the GSSO or CSSO must coordinate with gaining and losing PSMs or PSOs when eligibility concerns are identified.

12.12. DEBRIEFING ACKNOWLEDGMENTS.

a. The PSM or the PSO, or the GSSO or CSSO, as applicable, will implement a formal debriefing program when access to SAP information is no longer required, or an individual intends to or does travel to a country on the DoD SAPCO Consolidated Country Threat List.

b. Procedures for debriefing will be arranged to allow each individual the opportunity to ask questions and receive substantive answers from the individual providing the debriefing.

c. Security personnel at sites with access to JADE, or successor systems, will upload the debriefing acknowledgement into the database under the applicable program folder.

(1) Sites without access to the database, such as some industry locations, will forward the debriefing acknowledgement to the PSM or the PSO or designee within 3 business days.

(2) In cases where electronic processing of SAP personnel files is not executable due to contract requirements or infrastructure constraints, they will be submitted to the next level of operation until they can be properly filed in the official database of record.

d. SAP-accessed personnel will be debriefed by the PSM, the PSO, or the GSSO or CSSO, as applicable, or designee, and the personnel vetting access database will be updated to reflect this action.

e. The debriefing will include, at a minimum, a reminder of the individual's responsibilities as agreed to in the SAPIA, which addresses:

(1) The continuing obligations to not disclose SAP information.

(2) The SAPIA as an enforceable legal contract between the individual and the USG.

(3) All classified information, including SAP information, as the property of the USG.

(4) The penalties for espionage and unauthorized disclosure in accordance with Titles 18 and 50, U.S.C., concerning crimes and criminal procedure and war and national defense.

(5) The obligation not to discuss, publish, or otherwise reveal information about the SAP.

(6) Acknowledgement that all future questions or concerns regarding the SAP (e.g., solicitations for information, approval to publish material based on SAP knowledge or experience) will be directed to the PSM, the PSO, or the GSSO or CSSO, as applicable.

(a) Provide the individual with a telephone number for the PSM, the PSO, or the GSSO or CSSO, as applicable.

(b) Where to report suspected foreign intelligence service contacts or any attempt by unauthorized individuals to solicit SAP information. Information to be provided must include last known security officer's name and contact information. The priority for reporting this information is:

1. PSM or PSO.

2. GSSO (if applicable)

3. CSSO (if applicable).

4. Respective CI element or MDCO.

5. Nearest Federal Bureau of Investigation office.

(7) That each provision of the agreement is severable (i.e., if one provision is declared unenforceable by a court of competent jurisdiction, all others remain in force).

(8) Though an individual has signed the debriefing acknowledgment portion of the SAPIA, they are never released from the original SAPIA unless specifically notified in writing.

(9) The requirement to return all SAP, including classified, unclassified HVSACO, and CUI material, and the identification of all security containers to which the individual had access.

(10) How to obtain a security and policy review, in accordance with DoDIs 5230.09 and 5230.29, before publishing or other public release.

(11) What can and cannot be discussed or placed in resumes and applications for security clearances.

(12) The debriefing process, the requirement to sign the SAPIA, and the agreement that all questions about the SAPIA were addressed.

f. When access is suspended or revoked or an individual is debriefed for cause, the PSM, the PSO, or the GSSO or CSSO, as applicable, will notify that individual's CA SAPCO as listed in JADE or its successor system. The CA SAPCO will notify other CA SAPCOs holding interest in that individual's SAP accesses.

g. The individual conducting the debriefing will advise individuals who refuse to sign the debriefing acknowledgment portion of the SAPIA that such refusal may affect future access to SAPs or continued clearance eligibility.

(1) Refusal to sign the debriefing acknowledgement may be cause for administrative corrective actions, and it will be reported as a security incident to DCSA through the PSO.

(2) In the event that an individual refuses to execute a debriefing acknowledgement on the SAPIA, the GSSO or the CSSO must administer an oral debriefing in the presence of a witness and annotate the debriefing acknowledgment portion "ORAL DEBRIEFING CONDUCTED; INDIVIDUAL REFUSED TO SIGN." The briefer and witness sign beneath the statement attesting to this action.

(3) Refusal to sign will be reported immediately to the PSM or the PSO. The PSM or the PSO will promptly notify the GAM and the CA SAPCO.

12.13. ADMINISTRATIVE DEBRIEFINGS.

SAP security personnel must make every reasonable effort to debrief SAP-accessed individuals in person and have them sign a debriefing acknowledgement portion of the SAPIA. When that is not possible, individuals may be administratively debriefed.

a. If attempts to locate an individual either by telephone or mail are unsuccessful, and the whereabouts of the individual cannot be determined in no more than 30 days, the PSM, the PSO,

or the GSSO or CSSO, as applicable, must administratively debrief the individual by completing the debriefing acknowledgment portion of the SAPIA with "INDIVIDUAL NOT AVAILABLE – ADMINSTRATIVELY DEBRIEFED."

b. The appropriate database must be updated to reflect that the individual was administratively debriefed.

c. The PSM, the PSO, or the GSSO or CSSO, as applicable, must check to ensure that no SAP information is charged out to, or in the possession of, these individuals. If security personnel determine that the individual has retained information, they will immediately confer with the appropriate MDCO.

d. Except in cases where there is an exigent circumstance beyond the individual's control that is documented by the official executing the administrative debriefing, failure to debrief from a SAP will be documented in a memorandum for record that details the efforts outlined in Paragraph 12.13.a. and reported as a security incident to DCSA through the PSO.

12.14. SAP ACCESS SUSPENSION AND REVOCATION.

a. The PSM or the PSO, in consultation with the AAA, may suspend SAP accesses based on CA SAPCO guidance. The PSM or PSO will notify servicing legal counsel, human resources manager, security manager, and SSO (if applicable), as the situation dictates.

b. Local commanders and supervisors, in coordination with the CA SAPCO and the PSM or the PSO, must notify persons in writing when their eligibility or access has been suspended and include a brief statement of the reason(s) for the suspension of access consistent with the interests of national security. The notice will advise the subject that they may submit facts in writing that are relevant to the suspension reason(s) for consideration by the suspension official. The subject's commander, unit leader, or supervisor and the PSO will make a recommendation to the CA SAPCO on whether to revoke SAP access.

c. The CA SAPCO will make the determination regarding issuing a suspension or revocation of SAP access and will notify the subject through the commander, unit leader, or supervisor.

d. If the CA SAPCO suspends or revokes SAP access, the right to reconsideration and DoD SAPCO review processes in accordance with Paragraph 7.3. of this issuance will apply.

e. DoD Component heads and commanders, acting through their authorized representatives, must ensure access suspensions are reported to the appropriate adjudication facility via the DISS within the same calendar day as the suspension.

SECTION 13: SAPNP

13.1. INTRODUCTION.

The SAPNP provides a timely, standardized, program-level review of the nominated individual's package for access to a DoD SAP.

a. The SAPNP takes advantage of existing DoD resources and must ensure that nominated individuals meet three criteria:

(1) Final security clearance based on a favorable adjudication of an appropriate investigation.

(2) Demonstrated NTK.

(3) Access eligibility.

b. The SAPNP is not an investigation or adjudication. It is a standardized security management process that applies enhanced security procedures to determine personnel suitability for access to DoD SAPs.

(1) A PSQ must be completed to initiate the process.

(2) The nominated individual must provide additional information pertaining to each PSQ for which a "yes" response is provided.

(3) DoD SAPCO will provide a consolidated foreign intelligence threat list to assist PSMs, PSOs, GSSOs, and CSSOs in determining the risk associated with foreign affection, foreign association, and foreign travel.

c. Nominees who are U.S. citizens with additional citizenships in other countries, will be treated as U.S. citizens during the SAPNP. Nominees' reported foreign affections or foreign associates that have multiple citizenships will be treated as U.S. citizens during the SAPNP provided that at least one of their citizenships is U.S. Approval of SAP access for such persons does not require SecDef or DepSecDef approval. Nominees are required to declare any additional citizenship to another country (i.e., dual citizenship).

(1) PSMs and PSOs will fully assess unique risks with all suitability issues associated to the SAPNP.

(2) Risk assessments will not be based solely upon the nationality or country of origin of the individual and will be based on aggregated information to include CI and SAP threat assessments.

(3) Risk assessments should, at a minimum, identify risk(s) presented by a foreign entity, government, institution, organization, and/or person to information protected by SAP controls.

(4) PSMs and PSOs will use the risk assessment to make a recommendation to the AAA for the SAPNP.

(5) PSMs and PSOs must record any "Non-Concur" recommendation to the SAPNP in the SAP system of record, and the recommendation must include a documented risk assessment with a rationale for the action.

(6) AAAs will document and retain a summarized rationale for decisions that deny SAP access.

(7) AAAs who deny initial SAP access nominations will provide the PSO's risk assessment and the AAA's rationale to the nominating official. The nominating official may choose to cancel the nomination. However, to the extent consistent with national security, the nominating official may seek clarification or additional facts from the nominee and the nominating official may then choose to restart the nomination process, including the clarification or additional facts from the nominee.

13.2. NOMINATION REQUIREMENTS.

a. Candidates:

(1) Must be a U.S. citizen or dual U.S. citizen.

(2) Must possess a final TS or final SECRET clearance as appropriate to the SAP access requested.

(3) Must be enrolled in a DoD-compliant CV program.

(4) If nominated by a contractor, must have a valid and current DD Form 254 or consultant agreement authorizing SAP access in accordance with Part 117 of Title 32, CFR.

b. When the requirements of Paragraphs 13.2.a.(2) through 13.2.a.(4) cannot be met, requestor will submit an LOCN providing facts to support a determination that it is in the DoD's interest for the CA SAPCO to approve access.

c. Non-U.S. citizens' access to DoD SAPs will be evaluated in accordance with DoDD 5205.07 and Paragraph 3.13. of this issuance.

13.3. NOMINATION PACKAGES.

a. The PAR will be used to nominate an individual for SAP access. A single PAR may be prepared for multiple SAPs under the cognizance of the same AAA.

b. DoD and non-DoD personnel may only nominate other personnel for access to DoD SAPs, subordinate tiers, or portfolios the nominating individual is currently accessed to. Individuals are prohibited from self-nominating for SAP access.

c. The requestor will complete the PAR or provide the nominated individual's personal information, qualifications, and their NTK to the individual filling out the PAR.

d. All nomination packages for access to a DoD SAP will contain a PAR, a current PSQ completed within the last 365 days, supplemental information supporting "yes" answers on the PSQ, and for contractors, a current PSO-validated DD Form 254. Components will not create additional requirements in addition to those in this issuance unless the USD(I&S) approves an exception to policy. Refer to the September 20, 2021 DepSecDef Memorandum for approved exceptions.

e. The PSQ, and any supplemental information supplied by the nominated individual, will be maintained in an authorized SAP access management database (e.g., JADE or successor systems) and the personnel vetting file according to local SOP in accordance with Paragraph 12.6.

f. In support of a PAR for access to one or more SAPs, requestors will:

(1) Be accessed to the SAP and approved eligibility for access to the classification level for which the nominated individual is being submitted.

(2) Complete the PAR justification section, justifying why access is required and describing nominated individual's NTK.

(3) When a PAR cannot be completed by the requestor, a formal request will be submitted to the appropriate security office to be reviewed by the SPO. The request will include the nominated individual; program, tier, or portfolio being requested; justification; and the requestor's signature. The SPO will upload the formal request into the nominee's JADE, or successor system, file(s).

g. The SPO will be appointed in writing and will:

(1) Be responsible for the completeness and accuracy of information submitted in nominated individual's packages, based on information available to the SPO.

(2) Make initial eligibility determination or recommendation in accordance with this section.

(3) Be trained in their authorities, standards, and limitations in accordance with CA SAPCO guidance.

13.4. NOMINATION REVIEW PROCESS.

a. The DoD SAPCO, in coordination with the DCSA Center for Development of Security Excellence, will establish SPO training guidelines and curriculum. The SPO will:

(1) Be responsible for the completeness and accuracy of information submitted in the nominated individual's package based on information available to the SPO.

(2) Make initial eligibility determination or recommendation in accordance with this issuance.

b. The PSQ will be considered current and reciprocally accepted by all DoD Components if the questionnaire was completed within the last 365 days and there were no reportable changes since the PSQ was last completed.

(1) CA SAPCO may provide guidance to the SPO pertaining to processing PSQs with "Yes" responses.

(2) The CA SAPCO may require a LOCN.

c. The responsible SPO will review the nomination package for completeness and accuracy and will validate that the nominated individual meets the criteria in this issuance or requires additional review for SAP access.

(1) The SPO will check the approved security clearance database (e.g., DISS, Scattered Castles, or successor systems) to validate that the nominated individual has the appropriate clearance and the investigation completed date is current in accordance with DoDM 5200.02 and this issuance.

(a) The SPO will forward nomination packages via the PSM or the PSO to the appropriate CA SAPCO for decision to approve or continue access pending final disposition.

(b) Any DCSA decision to suspend or revoke the individual's eligibility for access to classified national security information supersedes the SAPNP.

(2) If the individual's investigation is not current, or the individual is not enrolled in a personnel vetting system, the SPO will refer the individual to their security manager or SSO to initiate the National Background Investigation Services eAPP "Questionnaire for National Security Positions."

(a) Once CE or CV is reflected in the approved security clearance database, the SPO will prepare the nomination package in accordance with Paragraph 13.4.

(b) The SPO will forward nomination packages via the PSM or the PSO to the appropriate CA SAPCO for decision to approve or continue access pending final disposition.

(c) Any DCSA decision to suspend or revoke the individual's eligibility for access to classified national security information supersedes the SAPNP.

(3) If the PSQ contains no potentially derogatory information, reflected by all "No" answers on the PSQ, no signature is required in the PSO block, and the SPO will make a recommendation to the GAM.

(a) PSOs will review the PAR, validate the candidate's NTK, and provide a concur or non-concur on the PAR.

(b) PSOs will forward the PAR to the AAA for an access approval determination.

(4) If the PSQ contains derogatory information, reflected by a "Yes" answer of the PSQ, the SPO will forward the PAR to the GAM for a NTK determination, and make a recommendation to the PSM or the PSO.

(a) GAMs will review the PAR, validate the candidate's NTK, and provide a concur or non-concur on the PAR.

(b) PSMs or PSOs will review the PAR and coordinate with intelligence and CI professionals from the DIA, MDCO, or DoD IC element to obtain current threat data to inform the access recommendation.

(c) PSMs or PSOs will provide sufficient justification in the PAR remarks for all instances of a non-concur that articulates the security, CI, or LE risk(s) or threat(s) associated to the derogatory information.

(d) PSMs or PSOs will record, retain, and protect specific information and intelligence that articulates the security, CI, or LE risk(s) or threat(s) associated to the derogatory information within approved databases and in accordance with all relevant intelligence-related laws or policies.

(e) PSMs or PSOs will forward the PAR to the AAA for an access approval determination and, upon request, provide the relevant and specific intelligence or threat information to the AAA, CA SAPCO, and DoD SAPCO.

(5) If the SPO determines that the answers to the PSQ qualify as previously unreported derogatory information, the SPO will refer the individual to their local security officer, who will report the new derogatory information to the DoD Consolidated Adjudications Services in accordance with DoDM 5200.02. The nomination process will proceed with the PSM or the PSO making a risk management decision based on the reported derogatory information.

d. The SPO may not disqualify a candidate for SAP access but may recommend additional review to the PSM or the PSO.

13.5. CONTINUED SAP ACCESS.

Continued SAP access is contingent on the individual's compliance with the following requirements:

a. SAP-accessed personnel have a responsibility to immediately report any changes in status that may affect their clearance eligibility in accordance with DoDM 5200.02 and the November 2, 2020 USD(I&S) Memorandum.

b. SAP-accessed personnel annually recertify answers provided to the PSQ or complete a new PSQ.

c. Failure to comply with reporting requirements or to update PSQs may result in suspension or revocation of SAP access.

d. GSSOs and CSSOs will instruct SAP accessed personnel to forward previously unreported derogatory information to their local security officer for submission to the DCSA. GSSOs and CSSOs will also notify servicing SSOs when the individual is accessed to SCI.

e. In support of personnel vetting program, the PSMs, the PSOs, the GSSO, the CSSOs and the SPOs will:

(1) Report derogatory information in DISS (or any successor personnel vetting system) that was disclosed in a PSQ, but not previously reported, to the candidate's organizational security manager, who will then create an incident report in DISS, or successor system.

(2) Cease processing of any PAR until it can be verified the owning organization reported this information and it was adjudicated by DCSA.

(3) Advise the individual of their responsibility to report derogatory information to their security manager as soon as they are aware of it.

13.6. DISAPPROVALS.

The AAA may disapprove nominated individuals for access by appropriately annotating and summarizing the reason for disapproval in the remarks section of the PAR.

a. All non-concur recommendations for accesses require additional justification in the PAR remarks section or must be provided in a separate memorandum.

b. Nominations disapproved for access may be resubmitted by the requestor. Any re-submission by the original requestor must include additional justification and be re-submitted to the same CA SAPCO.

c. All persons who receive a final corrective action determination impacting their access to DoD SAPs have the right to reconsideration of the decision in accordance with Paragraph 7.3. of this issuance.

SECTION 14: FOREIGN TRAVEL REPORTING

14.1. GENERAL.

SAP-accessed personnel must report official and unofficial foreign travel in advance and always be aware of their vulnerability to exploitation by foreign intelligence services. They are particularly susceptible during periods of foreign travel. Individuals must continuously exercise good judgment when traveling. Failure to comply with foreign travel reporting requirements in advance of the travel may result in suspension and possible loss of SAP access. Visiting foreign embassies located in the United States is considered foreign travel and will comply with foreign travel reporting requirements.

14.2. OFFICIAL GOVERNMENT BUSINESS TRAVEL.

a. SAP-accessed personnel will:

(1) In addition to reporting foreign travel to your activity security manager or facility security officer, inform the GSSO and the CSSO, as applicable, 14 business days in advance.

(a) If the 14-day requirement is not practical, the SAP-accessed traveler must provide written justification to the GSSO or the CSSO, as applicable, for coordination with the PSM or the PSO and organizational leadership approval.

(b) Notification must be provided in sufficient time to allow for the completion of an appropriate country-specific threat awareness briefing based on the DIA foreign intelligence threat level, MDCO, or CA SAPCO guidance.

(c) Pre-travel reporting will follow the established procedures established in the SOP and approved by the PSO. At a minimum, foreign travel notifications will include type of travel (official or unofficial), individual conducting travel, emergency contact information, destination, and mode of travel.

(2) Report any suspicious foreign contacts immediately upon return.

(3) Within 5 business days upon return, contact the GSSO or the CSSO, as applicable, to complete the SAPNP Template 3 and post-travel debriefing.

(4) The SAPNP Template 3 will be completed during the post-travel debriefing.

b. GSSOs or CSSOs will:

(1) Obtain the notification of foreign travel and other relevant documentation by the SAP-accessed traveler before leaving.

(2) Ensure personnel receive pre-travel threat awareness briefings and post-travel debriefings, using CI-support element provided products.

(3) Inform the PSM or PSO about any travel-related security issues identified by any SAP-accessed individual.

(4) File all completed documentation in the SAP-accessed traveler's personnel vetting file.

(5) Contact their designated PSM or PSO when personnel report unofficial foreign travel to countries identified as "high" on the element's country-specific threat matrix, or a travel advisory has been identified on the Department of State's Travel.State.Gov website. Flag these occurrences on the foreign travel reporting matrix.

c. PSMs or PSOs will:

(1) Upon request, support GSSOs or CSSOs with country-specific threat information to be used during foreign travel awareness briefings.

(2) As necessary, coordinate all CI-scope polygraph requests, additional inquiries, and investigations.

(3) Consult with their CI-support element when the CSSO or GSSO reports personnel taking unofficial foreign travel to a high-threat country, or a country under a travel advisory. Flag these occurrences on the foreign travel reporting matrix.

(4) Report suspicious travel incidents to their respective CI element or their supporting MDCO.

14.3. UNOFFICIAL TRAVEL.

a. SAP-accessed personnel will:

(1) Report anticipated foreign travel at least 30 days before the date of travel to the GSSO or the CSSO.

(a) If the 30-day requirement is not practical (validated reasons are determined by the responsible GAM, GSSO, or CSSO), the SAP-accessed traveler must provide written justification to obtain organizational leadership approval before leaving.

(b) Civilian air crew who are also briefed government employees will provide travel notification in advance by e-mail to their GSSO before airline travel. In-person travel debrief will be accomplished on their next government duty day.

(c) Pre-travel reporting will follow the established procedures in the SOP and approved by the PSO. At a minimum, foreign travel notifications will include:

1. Type of travel (official or unofficial).

2. Individual conducting travel.

3. Emergency contact information.

4. Date of travel.

5. Passport number, issuing country, and issuance and expiration dates.

6. Destination.

7. Mode of travel.

(2) Receive country-specific threat briefings from CI personnel based on DIA foreign intelligence threat level or CA SAPCO guidance. Same day travel must be reported immediately upon return.

(3) Report all suspicious foreign contacts immediately upon return.

(4) Contact the GSSO or CSSO to complete the notification of foreign travel debriefing within 5 business days upon return and complete a SAPNP Template, or successor reporting mechanism.

b. CSSOs or GSSOs will:

(1) Verify justification for travel requests reported with less than 30-day notice.

(2) Review all proposed foreign travel itineraries and in coordination with the PSM or PSO, request pre-travel, country-specific threat awareness briefings and post-travel debriefings from CI personnel from the supporting MDCO.

(3) Inform the PSM or PSO about any foreign travel, contacts, or security issues identified by any SAP-accessed individual.

(4) File all foreign travel requests in the SAP-accessed traveler's personnel vetting file.

(5) Report any foreign travel trends to the PSM or PSO. The travel information will be maintained in a readily accessible form (i.e., a spreadsheet or database).

c. The PSM or PSO will:

(1) Review justification for travel requests reported with less than 30-day notice given.

(2) When requested, coordinate with CI personnel from the supporting MDCO to provide country-specific threat awareness briefings and post-travel debriefings.

(3) Coordinate all CI-scope polygraph requests, additional inquiries, and investigations.

(4) Evaluate foreign travel trends by reviewing the aggregate of travel reported and entered into JADE, or successor systems.

(5) Report suspicious travel incidents to their respective CI element or their supporting MDCO.

14.4. INDIVIDUALS ASSIGNED TO FOREIGN COUNTRIES.

SAP-accessed personnel stationed in a foreign country are not required to report travel (official or unofficial) within that country.

a. Same day foreign travel to countries adjacent to the foreign country of station and not on the DoD SAPCO Consolidated Threat List must be reported immediately upon return.

b. All other foreign travel, including adjacent countries that are on the DoD SAP Consolidated Threat List will be reported in accordance with the requirements in Paragraphs 14.2 and 14.3.

14.5. FOREIGN TRAVEL RECORDS.

a. All completed foreign travel must be reported on the SAPNP Template 3.

b. All completed SAPNP templates will also be placed in the files section of the individual's record in JADE or its successor system.

c. Each SAP-accessed individual must inform the GSSO or CSSO, as applicable, of any suspicious foreign contacts encountered. The GSSO or the CSSO will notify the PSM or the PSO of all reports of suspicious foreign contact.

SECTION 15: PHYSICAL SECURITY PROCEDURES

15.1. GENERAL.

a. The procedures in this section are the standards for providing physical security for SAP information and materials in the DoD. Any additional requirements established by a DoD Component must be coordinated through the appropriate CA SAPCO for DoD SAPCO approval.

b. Other than as described in Paragraph 15.2., SAP information and materials may only be processed, handled (including manufacturing and testing), discussed, or stored in aa SAPF as described in this section. Systems, including weapons systems, containing SAP components may be employed and tested in open-air facilities not accredited as a SAPF when necessary as a part of their intended purpose, provided administrative procedures approved by the CA SAPCO are employed to protect them from unauthorized access or disclosure.

c. SAPFs will be accredited by SAPF-AOs designated by the CA SAPCOs. The applicable CSSO or GSSO is responsible for the daily operation of the SAPF and will notify the SAPF-AO of any activity that affects, or could affect, the accreditation. PSMs or PSOs may also serve as SAPF-AOs if designated by the CA SAPCO.

d. DoD contractors under the NISP must possess a facility security clearance (FCL) validated by the PSM or the PSO before a SAPF-AO may accredit a SAPF in their facility.

(1) The classification level of the SAP information within the SAPF cannot exceed the lower of the FCL classification level and the FCL safeguarding level.

(2) The CSSO or the GSSO will notify the PSM or the PSO of any activity that affects the FCL or SAPF accreditation.

e. All U.S.-accredited SAPFs may be utilized for any DoD SAPs up to the classification level for which the SAPF is accredited.

15.2. DISCUSSION, HANDLING, AND PROCESSING OF SAP IN AN ACCREDITED SCIF.

a. Acceptance of Existing Accreditation.

The CA SAPCOs may:

(1) Accept, instead of an accreditation as described in Paragraph 15.3. and without the co-utilization agreement (CUA) otherwise required, existing SCIF accreditations, and authorize the discussion, handling, and processing of SAP information and materials in private offices, and conferences rooms, within:

(a) Accredited permanent SCIFs, temporary SCIFs, and SCI secure working areas, as defined by Volume 2 of DoDM 5105.21, accredited by a DoD Component.

(b) Permanent SCIFs accredited, operated, and occupied by a non-DoD IC element.

(2) Make such an acceptance and authorization on a facility-by-facility basis, a Component-by-Component basis, a case-by-case basis, or otherwise.

(3) Issue SOPs on processing and handling SAP information within a SCIF.

b. Discussion.

When a CA SAPCO has accepted the accreditation of a SCIF in accordance with Paragraph 15.2.a., any DoD SAP may be discussed in a conference room or private office in that SCIF. Such use is at the discretion of the SCIF SSO, or designee, and must not interfere with the mission or, or activities taking place in, the SCIF.

(1) All individuals present in the private office or conference room must be accessed to the SAP or SAPs being discussed and must be U.S. citizens or SCI-indoctrinated citizens of Australia, Canada, New Zealand, or the United Kingdom. SAP accesses will be verified by the CA SAPCO.

(2) At least one individual in the discussion must be indoctrinated into the SCI compartments in use in the SCIF and be assigned to, or otherwise have an articulable nexus to, the SCIF or the organization resident in or with cognizance over the SCIF.

(3) At least one individual attending the meeting must be a resident of the organization space hosting the meeting and be briefed to all SAPs and subordinate tiers being discussed.

(4) At least one individual participating in, facilitating, or arranging the discussion must coordinate with the SCIF SSO, or designee, in advance of the discussion.

(5) Appropriate measures must be taken to ensure conversations cannot be overheard by non-briefed individuals.

(6) Any individuals participating in the discussion who are not indoctrinated to the SCI compartments in use in the SCIF must be escorted at all times by an individual authorized to escort in that SCIF.

c. Handling and Processing.

When a SAPCO has accepted the accreditation of a SCIF in accordance with Paragraph 15.2.a., SAP materials, including (with the approval of the SCIF SSO) standalone SAP IT that does not require a network connection (e.g., laptops, tablets, read books) may be introduced into and used in a conference room or private office in the SCIF in support of a SAP discussion as described in Paragraph 15.2.b.

(1) Approved SAP IT must have SSO and either PSM or PSO approval before the introduction of the equipment into the SCIF. Upon approval, equipment may be introduced into the conference room or private office and used in support of a SAP discussion occurring in accordance with Paragraph 15.2.b.

(2) SAP-accessed personnel may connect to non-persistent (access and local processing, but not local storage) SAP IT which is accessible over existing SCI networks in private offices or conference rooms in the SCIF to access and process SAP information. While processing is taking place, all individuals present in the office or conference room must be cross-briefed to the SAP or SAPs being accessed or measures must be taken to prevent inadvertent disclosure of SAP material, to include all non-briefed individuals leaving the room. Prior approval must be given by the CA SAPCO or designee before SAP processing can take place in identified offices or conference rooms.

(3) SAP materials may not be printed or stored in a SCIF, including in a private office or conference room, without complying with the requirements of Paragraph 15.1.c.

15.3. SAP-ACCREDITED AREAS.

a. Temporary SAPFs (T-SAPF), SAP compartmented area (SAPCA), SAPWA, and SAPTSWA are subtypes of SAPFs. Each type has different capabilities and is subject to different limitations.

(1) SAP information and materials may be processed, handled, discussed, and stored in a T-SAPF, SAPCA, or SAPF (that is not a SAPWA or SAPTSWA). A T-SAPF:

(a) May be accredited for a maximum of 12 months from the time of initial accreditation to de-accreditation. The 12-month allowance is not based on the amount of time the T-SAPF is used for the processing, handling, discussion, or storage of SAP information.

(b) May not be de-accredited and reaccredited to circumvent the 12-month limit. Extension requests must be submitted to the CA SAPCO.

(c) May not be accredited in a space that was accredited as a T-SAPF or SAPTSWA for more than 6 months in the past 2 years.

(2) SAP information and materials may be processed, handled, and discussed (but not stored) in a SAPWA or SAPTSWA. A SAPTSWA:

(a) May be accredited for a maximum of 12 months from the time of initial accreditation to de-accreditation, and may only be used to process, handle, or discuss SAP information and materials for a maximum of 40 hours per month.

(b) May not be de-accredited and reaccredited to circumvent the 12-month limit.

(c) May not be accredited in a space that was accredited as a SAPTSWA or T-SAPF for more than 6 months in the past 2 years.

b. The physical security safeguards established in the National Counterintelligence and Security Center (NCSC) "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities" (referred to in this issuance as the "NCSC SCIF Specifications") and the ICD 705 series are the physical standards for protection of SAP

information. Construction of SAPFs, T-SAPFs, SAPCAs, SAPWAs, and SAPTSWAs will conform to the equivalent facilities as defined in the NCSC SCIF Specifications in effect at the time the SAP area is initially accredited, unless variations are specifically noted in this issuance.

c. Security standards will apply to all proposed SAPFs and will be coordinated with the SAPF-AO for guidance and approval. Location of construction or fabrication does not exclude a SAPF from security standards or review and approval by the SAPF-AO.

d. The CA SAPCO must approve waivers for imposing safeguards that exceed standards outlined in ICD 705 series policy, even when the additional safeguards are based on risk.

e. A SAPCA is required when different compartmented programs are sharing the same SAPF, or when SAP is to be processed in a SCIF, and not all personnel are cross-briefed.

(1) CA SAPCO-designated SAPF-AO concurrence with visual, acoustic, and access control measures is required.

(2) Compartmented area personnel do not have to be briefed to the same program(s) as the normal operating level of the parent SAPF or SCIF. However, appropriate operating procedures must be approved by the responsible PSM or PSO(s) or GSSOs that ensure separation of non-cleared personnel from the various SAPs operating in the SAPF, SCIF, or the SAPCA.

f. Re-accreditation as a SAPTSWA requires a new physical inspection of the area.

15.4. RISK MANAGEMENT.

a. If, during the preconstruction and inspection phase, it is determined that full compliance with the minimum standards contained in this issuance is not possible, the SAPF-AO will recommend appropriate mitigating actions or activities based on analytical risk management process defined in NCSC SCIF Specifications.

(1) Such a waiver must include a robust risk mitigation plan that identifies how all unmet NCSC SCIF Specification requirements will be addressed through alternative mitigations to prevent the unauthorized disclosure of SAP information and must be approved in writing by the CA SAPCO.

(2) The CA SAPCO must provide DoD SAPCO with copies of all approved waivers.

(3) A SAPF accredited with such a waiver is not eligible for the discussion or handling of SCI in accordance with the November 30, 2023 Director of National Intelligence Memorandum.

b. SAPF-AOs must determine if a facility's security consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the SAPF.

(1) Security-in-depth (SID) describes the factors that enhance the probability of detection before actual penetration to the SAPF.

(2) The existence of a layer or layers of security that offer mitigations for risks may be accepted by the SAPF-AO.

15.5. PHYSICAL SECURITY PRECONSTRUCTION REVIEW AND APPROVAL.

SAPF-AOs will review physical security preconstruction plans for SAPF construction, expansion, or modification to ensure compliance with applicable construction and physical security standards in the NCSC SCIF Specifications. 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(s) from the NCSC SCIF Specifications for all SAP accreditations to the respective SAPF-AO for review and approval. The completed checklist will be classified in accordance with specific SAP security classification guidance.

b. A TEMPEST countermeasure review is required for all SAPFs and will be provided by a certified TEMPEST technical authority (CTTA). A technical surveillance countermeasures (TSCM) review of the physical security pre-construction plan is recommended for mitigation strategies against current technical foreign intelligence threats.

c. Major renovations to the SAP-accredited area, as determined by the SAPF-AO, will result in the SAP-accredited area being required to comply with the version of the NCSC SCIF Specification in effect at the time of the renovation, rather than the version in effect at the time the area was originally accredited.

15.6. SAP CONSTRUCTION PROCEDURES.

a. The SAPF-AO will:

(1) Review and approve or disapprove the design concept, construction security plan, and final design for each construction project before the start of construction in accordance with the NCSC SCIF Specifications and this issuance. Refer to NCSC SCIF Specifications for all construction standards.

(2) Physically inspect a SAPF before accreditation in accordance with construction standards in the NCSC SCIF Specifications and this issuance.

(a) Photographs will be taken during all phases of construction to document relevant specification compliance and serve as part of the accreditation packet. If the SAPF is being constructed in an area where photography is restricted (e.g., within a SCIF or within the Pentagon), adhere to all applicable policies for photography permits and reviews and approvals.

(b) Photographic evidence can assist PSMs or PSOs in revalidating fixed facility checklists (FFCs), validating new construction, and demonstrating compliance to tenant units within CUAs.

(3) Inspect SAPF at an interval determined by the CA SAPCO and, in coordination with the PSM or PSO, withdraw accreditation when situations dictate.

(4) Approve and document mitigations commensurate with the standards in the NCSC SCIF Specifications.

(5) Recommend waivers of physical security safeguards to the CA SAPCO.

(6) Ensure mitigating strategies are implemented and documented in the construction security plan in the NCSC SCIF Specifications when using non-U.S. citizen workers.

(7) When deemed necessary, request construction surveillance technicians to supplement site access controls, implement screening and inspection procedures, and monitor construction and personnel in accordance with NCSC SCIF Specifications. A TSCM survey of the site to augment construction surveillance is recommended to assist with identifying technical CI risks.

b. The PSM or PSO will physically inspect the SAPF in accordance with ICD 705 standards and report any deficiencies to the SAPF-AO.

(1) If deficiencies are identified, the affected organization will develop a corrective action plan, which the PSM or PSO will oversee until all ICD 705 standards have been met.

(2) Once all ICD 705 standards have been met, the PSM or PSO will forward a final report to the SAPF-AO for review and concurrence.

c. The site security manager, as defined in the NCSC SCIF Specifications, will:

(1) Advise the SAPF-AO of the potential for variation from the requirements of this issuance.

(2) In consultation with the SAPF-AO, develop a construction security plan regarding implementation of the standards of this issuance and the NCSC SCIF Specifications. The site security manager will submit a plan of actions and milestones to be approved by the SAPF-AO to document all security related actions and milestones during the construction of the SAPF. This includes but is not limited to the establishment of site security measures, document preparations such as the construction security plan, pre-construction checklist, and FFC, photographs to be taken and at what stages or intervals, and site inspections.

(3) Conduct periodic security inspections for the duration of the SAPF construction to ensure compliance with the construction security plan.

(4) Prepare necessary waiver requests and forward to the SAPF-AO for further processing.

(5) Investigate and document security violations or deviations from the construction security plan. If violations or deviations are found, the site security manager will notify the PSM or the PSO of security violations and the SAPF-AO of deviations from the construction security plan within 24 hours of incident detection.

(6) Implement physical access control measures in accordance with the NCSC SCIF Specifications.

d. The CTTA will:

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

(2) Provide the SAPF-AO with documented results of the review with recommendations. In accordance with CNSS Instruction 7000, when a recommended countermeasure is not implemented, the CA SAPCO, or designee, must accept the risk in writing.

e. Ensure construction security requirements are detailed in the NCSC SCIF Specifications and this issuance.

15.7. ACCREDITATION.

a. The procedures for establishment and accreditation of a SAPF will follow guidelines distributed by DoD SAPCO.

b. The SAPF-AO will inspect any area before accreditation as any type of SAPF.

c. 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.

d. Announced or unannounced inspections may occur at any time.

e. The current FFC will be reviewed during inspections to ensure continued compliance.

f. TSCM evaluations may be required at the discretion of the SAPF-AO, as conditions warrant, and will be implemented in accordance with DoDI 5240.05.

g. Inspection reports will be retained within the SAPF and by the SAPF-AO in accordance with records management plans.

h. All SAPFs will have on site current copies of:

(1) SAPF FFC and supporting documentation, to include photos of the construction process. Photos should be retained for the life of the facility.

(2) Any accreditation documents (e.g., physical, TEMPEST, and ISs) 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 accreditation.

(5) Operating procedures and any security documentation, including IS security authorization packages, CUAs, appointment letters, MOAs, and emergency action plans.

15.8. CUA AND CO-ACCREDITATION.

Co-utilization occurs when a SAPF is used for the processing, handling, discussion, or storage of SAP information under the cognizance of two or more CA SAPCOs. Co-accreditation is when a space is accredited as both a SAPF and a SCIF, allowing for the processing, handling, discussion, and storage of both SAP and SCI in the same facility.

a. The CUA documents areas of authorities and responsibilities between two or more organizations that share the same SAPFs.

b. A CUA for co-utilization of SAPFs or by non-DoD agencies will be executed between the two organizations. SAP CUAs between the same organization should not be required beyond a written communication outlining primary host and tenant responsibilities.

(1) Unless otherwise agreed upon, the first organization in an area will be considered the host responsible for all security oversight. Security oversight in this context means responsible security agency for physical security of the overall facility requiring sole authority responsibility for related physical security requirements but ensures coordination with the other entity.

(2) The CUA will be initiated by the organization desiring to co-use a space and will be approved by both PSMs or PSOs and the GAM or CAM, unit commander, or appropriate industry official for both organizations before introduction of the additional SAP(s) into the SAPF.

c. At a minimum, CUAs must include:

(1) Compliance inspection responsibility.

(2) Incident notification.

(3) Host-tenant agreement clarifying inspection responsibilities.

(4) The CUA template annotated in accordance with the NCSC SCIF Specifications.

d. CUAs will remain in effect until cancelled by the host or tenant activity, in writing. A CUA between contractors and the USG will be cancelled at the end of the period of performance for either the host or tenant.

e. The host unit will keep all tenant activities informed of all waivers to the requirements of this issuance throughout the life of the CUA, to include any changes to compensatory measures or mitigating controls put in place for the waivers.

f. If the SAPF being co-used is a SAPCA located within a parent SCIF or is co-accredited as a SCIF, the DoD Components that agree to SAPF CUAs will forward a courtesy copy to the SCIF-accrediting Component after the CUA is made and ensure the CUA is uploaded to the SAPF system of record.

g. DoD Components that agree to CUAs with departments or agencies also authorized to establish SAPs will forward a courtesy copy to DoD SAPCO and ensure the CUA is uploaded to the SAPF system of record.

h. Agencies desiring to co-utilize a SAPF will accept the current accreditation of the cognizant agency if the SAPF was accredited without waiver to the standards in this issuance.

(1) Prospective tenants will be informed by host organization of all mitigations and waivers to the requirements of this issuance before co-utilization and keep all tenants informed of all waivers throughout the life of the CUA, to include any changes to compensatory measures or mitigating controls put in place for the waivers.

(2) Any security enhancements required by other departments or agencies 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 approved by all parties to the agreement.

i. When a space, or part of a space, is to be used for both SCI and SAP information, it must be accredited as a SAPF in accordance with this issuance and as a SCIF in accordance with ICD 705.

(1) Co-accreditation also requires a CUA to ensure each accreditor is aware of the facility's use for the other's information.

(2) Authorization from the SSO and either the PSM or PSO is required before establishing:

(a) A SCIF within a SAPF.

(b) A SAPCA within a SCIF.

(c) An SCI CA within a SAPF that is either itself located within a SCIF or is co-accredited as a SCIF.

j. A CUA must be established before occupancy.

15.9. PHYSICAL ACCESS CONTROLS.

a. Only assigned SAP-indoctrinated personnel will have unescorted access to a SAPF. Where practicable, GSSOs and CSSOs should maintain access rosters for all personnel who have unescorted access to a SAPF.

b. Each SAPF will have procedures for identification and control of visitors seeking physical access in accordance with this issuance and NCSC SCIF Specifications. Personal introduction and identification should be used to the maximum extent.

c. The PSM or PSO may require a badging system when all individuals within a SAPF cannot personally identify those with access. This normally occurs when a SAPF hosts more than 25 people.

(1) When a badge system is considered necessary, it will be documented in the SOP 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 PSM or the PSO or the GSSO may negate the requirements in this section for badge inventory, accountability, and destruction.

(3) Badge systems used for access control to USG-controlled, SAP-accredited areas must comply with Homeland Security Presidential Directive 12. The use of badges other than the personal identity verification card is permitted for circulation control within SAP-accredited areas.

d. When not occupied, SAPFs will be alarmed in secure mode and secured with an approved General Services Administration FF-L-2740A combination lock in accordance with Federal Specification FF-L-2740B.

e. Access control to a SAPCA will be accomplished by mechanical or electronic access control devices only.

(1) Spin-dial combination locks (e.g., XO series locks) are prohibited on SAPCA doors, and independent alarm systems will not be installed in a SAPCA; however, a zone from the parent intrusion detection system may be installed in the SAPCA with a separate keypad.

(2) Intrusion sensors will be installed when the SAPCA includes an exterior boundary wall of the parent SAPF or SCIF.

f. Emergency personnel or first responders and their equipment (including devices carried by emergency medical personnel) responding to a medical or security (police) crisis within a SAPF will be admitted without regard to their security clearance status.

(1) Emergency personnel or first responders will be escorted to the degree practical.

(2) Arrangements will be made for the debriefing of emergency personnel or first responders as soon as possible.

15.10. CONTROL OF COMBINATIONS.

a. Combinations to locks will not be the same throughout a SAPF (e.g., doors, vaults).

b. Combinations to locks installed on security containers, 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 PSM, the PSO, the GSSO, or the CSSO 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

(3) The DoD Lock Program is designated as the DoD technical authority for locking and storage systems used for the protection of classified information. For technical support, call the DoD Lock Program Technical Support Hotline at 1-800-290-7607 or DSN 551-1212 or review the website at https://www.navfac.navy.mil/navfac_worldwide/specialty_centers/exwc/products_and_services/capital_improvements/dod_lock.html.

d. All combinations to the SAPF entrance doors will be recorded on the Standard Form 700, "Security Container Information," (available at https://www.gsa.gov/reference/forms/security-container-information) and stored in a different SAPF accredited at the same or higher classification level and handling caveat. When this is not feasible, the PSM or PSO or GSSO will prescribe alternative storage locations.

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

15.11. ENTRY-EXIT INSPECTIONS.

The SAPF will have procedures for inspecting personal belongings and vehicles at the entry and exit points, or at other designated areas.

a. Inspections will deter the unauthorized removal of classified material and the introduction of prohibited items.

b. Legal counsel will review all personnel inspection procedures before implementation.

15.12. CONTROL OF ELECTRONIC DEVICES AND OTHER ITEMS.

a. The facility SOP will contain guidance for control of portable electronic devices (PEDs) and other items introduced into or removed from the SAPF in accordance with ICD 124. Unclassified PEDs that store, record, or transmit information are generally prohibited in SAPFs. PEDs that do not meet the exceptions of Paragraphs 15.12.b. or 15.12.c. require review and approval by the SAPF-AO and ISSM or senior information security officer (SISO) before being brought into a SAPF.

b. PEDs that do not store, record, or transmit information (e.g., electronic calculators, receive-only pagers, and radios) are authorized within SAPFs. PEDs that have minimal transmission capabilities (e.g., car key fobs) but not user accessible storage or camera, microphone, cellular, Bluetooth, or Wi-Fi capabilities are authorized within SAPFs.

c. Personal fitness devices (e.g., step counters, health rings) that do not contain user-accessible storage and that do not contain microphone, camera, cellular, or Wi-Fi capabilities are authorized within SAPFs.

d. Processes will consider any risks with SAR ISs operating within the same space.

e. See Table 1 for collaboration peripherals in SAPFs.

f. Wireless capabilities in SAPFs are subject to ODNI policy on wireless capabilities in SCIFs, as described by the January 19, 2017 Director of National Intelligence Memorandum and its implementing policies and standards.

Table 1. Summary of Collaboration Peripherals in SAPF DoD Secure Spaces

Peripheral	Permissions
Privately-owned headsets, microphones, and webcams	Prohibited.
Wireless headsets, microphones, or webcams	Prohibited.
Built-in microphones or webcams	Prohibited on unclassified computers. May be authorized on classified computers, subject to approval by the Component chief information security officer with cognizance of the computer or device, and potential restriction from the SAPF-AO that accredited the SAPF.
Government-issued wired external microphones	May be authorized on unclassified devices only when equipped with push-to-talk capability or a technology services group-approved positive disconnection device that operates by physical means. May be authorized on classified computers, subject to approval by the Component chief information security officer with cognizance of the computer or device, and potential restriction from the SAPF-AO that accredited the SAPF.
Government-issued wired external webcams	Prohibited on unclassified computers. May be authorized on classified computers, subject to approval by the Component chief information security officer with cognizance of the computer or device, and potential restriction from the SAPF-AO that accredited the SAPF.
Government-issued wired external headset without a microphone	Authorized.

g. Electronic medical devices (EMDs) require review and approval by the SAPF-AO, ISSM, or SISO before being brought into a SAPF. Generally, EMDs that store, record, or transmit information provided the device has no ability to capture information from the surrounding environment (e.g., it stores, records, and transmits only heart-related or glucose-related information and has no user-accessible storage or camera or microphone capability) are approved. Medical devices approved for access into SCIFs will be accepted into SAPFs.

(1) When reviewing multi-component medical devices consisting of one or more components that do not contain prohibited capabilities and one or more components that do (e.g., continuous glucose monitors, insulin delivery pods, heart monitors or EKG units, and implanted pacemakers that pair with purpose-built devices or applications on smartphones that monitor, display, or wirelessly relay health information to a health care provider), the SAPF-AO, ISSM, or SISO should approve the components that do not contain prohibited capabilities. Components that contain prohibited capabilities are prohibited in SAP accredited areas.

(2) The SAPF-AO, ISSM, or SISO will seek human resources and legal guidance before denying any medical device.

(3) Further guidance for EMDs is defined in ICD 124.

h. Prohibited PEDs must be stored outside the SAPF. In instances where a SAPF perimeter is also a building perimeter and a non-discussion lobby area exists, and storage outside the building would create an antiterrorism threat or a mass casualty event chokepoint, the SAPF-AO and PSM or PSO may jointly designate an area at the entry point to the SAP-accredited area for the storage of PEDs. Where PED storage areas are allowed to be within the SAP-accredited area, the PEDs will be turned off and stored in opaque, sealed containers. These designated PED storage areas will be confined to designated "non-discussion" areas.

i. Mission-essential government- or contractor-owned PEDs introduced into the SAPF-will be approved by the PSM or PSO and SAPF-AO or designee in accordance with the NCSC SCIF Specifications before entering the SAPF.

(1) The GSSO or the CSSO will establish SOPs for notification that such equipment is being brought into the SAPF for PSM or PSO and SAPF-AO review and approval.

(2) The SOP will consider any risks with SAR ISs operating within the same space.

j. Waivers to this policy must be submitted by the SAPF-AO in writing, approved by the CA SAPCO or designee, and a copy provided to the DDI(CL&S). These requests will:

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

(2) Be coordinated with the appropriate AO for each affected IS within the SAP-accredited area.

(3) Identify mitigations.

(4) Identify risks after mitigation to classified information.

k. Any SAPF with one or more approved waivers must revise its SOP to define the procedures and guidance for control of PEDs and other items introduced into or removed from the SAPF. In addition, any tenant SAP PSMs or PSOs will be notified in writing and informed the facility is accredited with waiver for appropriate action by the tenant CA SAPCO.

l. EMDs in SAPFs located within SCIFs will comply with ICD 124.

15.13. TEMPEST REQUIREMENTS.

a. When meeting TEMPEST standards is required, the SAPF-AO, or PSM or PSO in coordination with the SAP-AO, 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 the NCSC SCIF Specifications and CNSS Instruction 7000.

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 SCI contracting official should be implemented. The processing of classified national security information as defined in Volume 3 of DoDM 5200.01 or the submission of information for a TEMPEST countermeasure review does not imply a requirement to implement TEMPEST countermeasures, but TEMPEST countermeasures should be considered when electronic processing occurs. TEMPEST countermeasures that CTTA may recommend include, but are not limited to:

(1) The use of shielded sections 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 CNSS Advisory Memorandum TEMPEST/01-13.

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.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AAA	access approval authority
AO	authorizing official
ATO	authority to operate
CA	cognizant authority
CAM	contractor activity manager
CAP	controlled access program
CE	continuous evaluation
CFA	core functional area
CFR	Code of Federal Regulations
CI	counterintelligence
CMP	consequence management plan
CNSS	Committee on National Security Systems
COA	continuation of access
CPI	critical program information
CSSO	contractor special access program security officer
CTTA	certified TEMPEST technical authority
CUA	co-utilization agreement
CUI	controlled unclassified information
CV	continuous vetting
DCIO	Deputy Chief Information Officer
DCSA	Defense Counterintelligence and Security Agency
DD	Department of Defense (form)
DDI(CL&S)	Director for Defense Intelligence (Counterintelligence, Law Enforcement, and Security)
DepSecDef	Deputy Secretary of Defense
DIA	Defense Intelligence Agency
DISS	Defense Information System for Security
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
DPEP	Defense Personnel Exchange Program
DSN	Defense Switched Network
EKG	electrocardiogram
EMD	electronic medical device
E.O.	Executive order

ACRONYM	MEANING
FCL	facility security clearance
FFC	fixed facility checklist
FWAC	fraud, waste, abuse, and corruption
GAM	government activity manager
GCA	government contracting activity
GSSO	government special access program security officer
HVSACO	handle via special access channels only
IC	Intelligence Community
ICD	Intelligence Community directive
IP	intellectual property
IR&D	independent research and development
IS	information system
ISSM	information system security manager
IT	information technology
JADE	Joint Access Database Environment
JSIG	Joint Special Access Program Implementation Guide
JWICS	Joint Worldwide Intelligence Communication System
LE	law enforcement
LOCN	letter of compelling need
MDCO	Military Department counterintelligence organization
MOA	memorandum of agreement
NCCS	National Industrial Security Program Contract Classification System
NCSC	National Counterintelligence and Security Center
NISP	National Industrial Security Program
NSA/CSS	National Security Agency/Central Security Service
NSS	national security system
NTK	need to know
OA	oversight authority
OCA	original classification authority
ODNI	Office of the Director of National Intelligence
OPR	office of primary responsibility
OPSEC	operations security
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security

ACRONYM	MEANING
PAR	program access request
PED	portable electronic device
PID	program identifier
PPP	program protection plan
PSA	Principal Staff Assistant
PSM	program security manager
PSO	program security officer
PSQ	pre-screening questionnaire
SAP	special access program
SAPCA	special access program compartmented area
SAPCO	special access program central office
SAPF	special access program facility
SAPF-AO	special access program facility accrediting official
SAPIA	special access program indoctrination agreement
SAPNP	special access program nomination process
SAPTSWA	special access program temporary secure working area
SAPWA	special access program working area
SAR	special access required
SAV	staff assistance visit
SCG	security classification guide
SCI	sensitive compartmented information
SCIF	sensitive compartmented information facility
SecDef	Secretary of Defense
SEI	special emphasis item
SETA	security education and training awareness
SID	security-in-depth
SISO	senior information security officer
SOP	standard operating procedure
SPO	special access program personnel vetting official
SSO	special security officer
T-SAPF	temporary special access program facility
TS	TOP SECRET
TSCM	technical surveillance countermeasure
U.S.C.	United States Code
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USG	U.S. Government
USPS	United States Postal Service

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
AAA	A government employee authorized to make approval and disapproval decisions for personnel nominated for access to DoD SAPs. This person may be the OA, CA SAPCO, or a properly trained designee appointed by same.
access	Defined in Section 6.1.(a) of E.O. 13526.
Access National Agency Check and Inquiries	The minimum initial investigation for civilian personnel applying for non-critical sensitive national security positions. This is a legacy investigation which may be encountered in PCL database.
accreditation	The formal approval of a specific place, referred to as a SAPF, that meets prescribed physical, technical, and personnel vetting standards.
administrative debriefing	The act of removing someone from SAP access and documenting this status due to the inability of the government to have the individual formally debriefed and physically sign the debriefing section of the SAPIA.
AO	Individual that assumes responsibility for operating an IS at an acceptable level of risk to agency operations within the DoD ATO process, as described by the National Institute of Standards and Technology's Risk Management Framework.
archive	Defined in DoDI 5205.11.
ATO	Authorization granted by an AO for a DoD IS to process, store, or transmit information; an ATO indicates a DoD IS has adequately implemented all assigned cybersecurity controls to the point where residual risk is acceptable to the AO.
billet	A determination that, in order to meet NTK criteria, certain SAPs may elect to limit access to a predetermined number of properly cleared employees.

TERM	DEFINITION
CAM	The contractor individual responsible for management of SAP(s) at the contractor location.
CI-scope polygraph	A screening polygraph examination that uses relevant questions limited to prescribed CI issues.
COMMENDABLE	A rating assigned to a contractor or government location that has implemented security requirements in an effective fashion resulting in a generally robust security posture. This rating denotes a security program with strong management support, exemplary practices, and the absence of any serious security issues.
compromise	An unauthorized disclosure of classified information.
condition	Access eligibility granted or continued with the provision that additional security measures will be required. Such measures include, but are not limited to, additional security monitoring, access restrictions, submission of periodic financial statements, and attendance at counseling sessions.
corrective action plan	A document that addresses the plan for correcting deficiencies and areas deemed unsatisfactory as noted in the self-inspection report.
co-utilization	The use of the same SAPF by two or more organizations; a SAPF used for two or more SAPs; or for a SCIF dual-designated as SAPF.
CPI	Defined in DoDI 5200.39.
CSSO	The contractor individual designated in writing by the CAM who will provide security administration and management for a SAP at a cleared defense contractor location.
CTTA	Defined in CNSS Policy 300.

TERM	DEFINITION
deviation (personnel)	Access eligibility granted or continued despite either a significant gap in coverage or scope in the investigation or out-of-date investigation. "Significant gap" for this purpose means either complete lack of coverage for a period of 6 months or more within the recent 5 years investigated or the lack of a Federal Bureau of Investigation name check or technical check, or the lack of one or more relevant checks.
deviation (process)	Undocumented, or documented and not complied with, procedures that if left uncorrected could cause increased risk of loss or compromise of classified information. This could include administrative issues that could result in multiple deviations; trends; or repeat deviations may result in a finding as they pertain to compliance inspections.
disinterested party	An individual accessed to the SAP(s) who is not the custodian of the accountable item being reviewed and is not within the direct supervisory chain of the custodian.
DISS	System used to track personnel security clearances.
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.
foreign affection of foreign associate	A close and continuing relationship with a foreign national that involves a bond of affection, influence, common interests, or obligation. This relationship can occur between a foreign national and an applicant, their spouse, or cohabitant.
GAM	The appointed individual responsible for managing assigned SAP(s). The GAM assumes the responsibility for overall security management of assigned SAPs. Often, the GAM is the organization's commander or director, though not always.

TERM	DEFINITION
GCA	A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. The term includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer.
GSSO	A fulltime government position within the security career profession, appointed in writing at a government SAPF or organization by the Director or GAM, to provide security administration and management.
inadvertent disclosure	The unintentional disclosure of classified SAP or HVSACO information to an individual without authorization to access the disclosed SAP information.
incident	Instances when personnel do not fully adhere security policies or procedures, which are categorized as infractions or violations in accordance with Volume 3 of DoDM 5200.01.
infraction	Defined in Volume 3 of DoDM 5200.01.
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 and characterizes the incident as an infraction or a violation. The inquiry identifies, if possible, the cause(s) and person(s) responsible, reports corrective action or recommends a more in-depth investigation. Generally, inquiries are initiated and conducted at the lowest level possible.
inspector	For inspections of government and contractor activities, the government official with the authority to conduct SAP external inspections within their agency or organization. For subcontractors, the representative of the prime contractor with the authority to inspect the subcontractor.

TERM	DEFINITION
investigation	Examination conducted by an element with official investigative authority 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.
IP	Defined in DoDI 5010.44.
issue-based polygraph examinations	An issue-based polygraph examination that is predicated on an allegation or a specific issue under investigation.
LOCN	A written description of an individual's unique skills or knowledge, the benefit the SAP will gain by accessing the individual, and why no other individual can fulfill or is readily available to fulfill that position. Normally included within Block 35 ("Justification") of a PAR, a LOCN can also be a signed and dated memorandum from the CA SAPCO granting an exception to the requirement concerned.
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 rating assigned to a contractor or government location that has implemented security requirements in an ineffective fashion, resulting in an unreliable security posture. This rating denotes a serious finding in one or more security areas that could contribute to the eventual compromise of classified information if left uncorrected.
mitigation measures	Equivalent protective measures used only after determining that the exact requirements of this issuance cannot be met. Equivalent levels of protection will not be designed with the intent to reduce or lessen the security requirements of this issuance.

TERM	DEFINITION
National Agency Check with Law and Credit	The minimum initial investigation for military accessions and contractor personnel that require eligibility for a CONFIDENTIAL or SECRET security clearance. This is a legacy investigation which may be encountered in PCL database.
NTK	A determination that a prospective recipient requires access to specific classified information 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).
opaque container	A container that fully obstructs the visibility of its contents and prevents the surrounding area from being visible by its contents.
personnel vetting	The security discipline that assesses the loyalty, reliability, and trustworthiness of individuals for initial and continued eligibility for access to classified information or assignment in sensitive positions.
phased periodic reinvestigation	A periodic reinvestigation of limited scope used in lieu of a single scope background investigation.
portfolio	An access management tool that DoD SAPCO establishes and is the AAA for groups of two or more SAPs, usually by topic or mission area.
PSM	A government or government support position within the security career profession, appointed in writing by the appropriate Director, CA SAPCO or designee, that has the responsibility for managing subordinate PSOs in accordance with the activity structure, program mission scope, and level of effort established by the Component.

TERM	DEFINITION
PSO	A government position within the security career profession, appointed in writing by the appropriate Director, CA SAPCO or designee, who is responsible for executing oversight and ensuring SAP security requirements for a specific SAP, group of SAPs, geographical assigned locations, or agency or organization(s) are being executed. The PSO ensures security functions are being executed in accordance with applicable legal, regulatory, and policy requirements and works in tandem with GAMs, CAMs, GSSOs, and CSSOs. There are three categorizations of PSOs: PSO, appointed to a specific program or sub-compartment or project to ensure security oversight of the program. Geographical PSO, appointed to specific geographical locations to ensure program security support to program PSOs. Organizational PSOs, appointed to a specific agency or organization or multiple organizations to ensure program security support to program PSOs.
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.
requestor	An individual who is currently program briefed and requests SAP access for an individual not higher than the classification level and SAPs that the requestor is assessed to, and completes the justification section of the PAR.
revocation of SAP access	Rescinding SAP access when a currently SAP-accessed individual is determined to be ineligible.

TERM	DEFINITION
risk management	The process that allows PSMs or 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.
SAPCA	A room or set of rooms located within a SAPF or SCIF that is designed to protect activities occurring at different SAP levels or with different PIDs. A SAPCA is required when different compartmented programs are sharing the same SAPF or SCIF and when not all personnel are cross-briefed.
SAPF	Defined in DoDI 5205.11.
SAPF-AO	An official designated by a CA SAPCO who is authorized to accredit DoD SAPFs according to standards in ICD 705 and any supplemental CA SAPCO SOPs.
SAP umbrella	Defined in DoDI 5205.11.
SAPWA	An accredited area where the discussion and non-persistent processing of SAP information is authorized. No storage is authorized.
SAPTSWA	An accredited area where the discussion and non-persistent processing of SAP information is authorized on a short-term (12-month maximum) basis. Use is limited to 40 hours per month.
SATISFACTORY	A rating assigned to a contractor or government location that has implemented security requirements in an effective fashion, resulting in a fundamentally reliable security posture. This rating is the most common and it denotes that a security program is in general conformity with basic requirements and does not have any serious security issues.
Scattered Castles	Defined in Intelligence Community Policy Guidance 704.5.
SCI	Defined in ICD 703.

TERM	DEFINITION
SCIF	An accredited area, room, group of rooms, building, or installation where SCI may be stored, used, discussed, or electronically processed.
self-inspection	A physical verification by the owning agency or organization of the security processes, procedures, and administrative documentation that support the SAP.
SETA	Defined in Enclosure 6 of Volume 3 of DoDM 5105.21.
SID	A determination made by the SAPF-AO that a facility's security 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 SAPF-AO as adequate.
single scope background investigation	The minimum investigation for personnel applying for special or critical sensitive national security positions or for personnel that require eligibility for a TS security clearance.
site security manager	The primary POC for construction projects who interfaces directly with the AO throughout the planning and design processes. Responsibilities are defined in the NCSC SCIF Specifications.
SPO	Individual that has been trained and approved to apply enhanced security procedures to determine personnel eligibility for access to DoD SAPs in accordance with this issuance.
suspension of access	An action taken in accordance with Paragraph 7.2 to temporarily withdraw the access of a currently SAP-accessed individual as a result of certain personnel vetting conditions or questionable circumstances, pending the resolution of an investigation or inquiry.

TERM	DEFINITION
system of record	Defined in the Privacy Act.
technology transfer	Defined in DoDI 5535.08.
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 the NCSC SCIF Specifications.
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 evaluation	A physical, electronic, and visual examination to detect technical surveillance devices, technical security hazards, and attempts at clandestine penetration.
umbrella SCG	A SCG is issued by the Director, DoD SAPCO and developed by incorporating information common to all subordinate tiers within the SAP hierarchy, as defined in DoDI 5205.11. Umbrella SCGs are supplemented by annexes, the purpose of which is to identify CPI within each umbrella's subordinate tier.
UNSATISFACTORY	A rating assigned to a contractor or government location that has failed to implement baseline security requirements, resulting a defective security posture. This rating denotes serious findings and conditions where the location has lost, or is in imminent danger or losing, its ability to adequately safeguard the classified material in its possession or to which it has access.
violation	Defined in Volume 3 of DoDM 5200.01.
waiver	An exemption to the security requirements of this issuance.

REFERENCES

Code of Federal Regulations, Title 32, Part 117

Committee on National Security Systems Advisory Memorandum TEMPEST/01-13, "RED/BLACK Installation Guidance," January 17, 2014[1]

Committee on National Security Systems Instruction 1253, "Categorization and Control Selection for National Security Systems," July 29, 2022

Committee on National Security Systems Instruction 5000, "Voice over Internet Protocol (VoIP) Telephony," August 2, 2021

Committee on National Security Systems Instruction 7000, "TEMPEST Countermeasures for Facilities," May 2004

Committee on National Security Systems Instruction 7003, "Protected Distribution Systems (PDS)," September 2015

Committee on National Security Systems Policy 22, "Cybersecurity Risk Management," September 2021

Committee on National Security Systems Policy 300, "(U) National Policy on Control of Compromising Emanations," April 2004

Deputy Secretary of Defense Memorandum, "Exception to Policy for Submission of a Pre-Screening Questionnaire," September 20, 2021[2]

Directive-type Memorandum 22-001, "DoD Standards for Records Management Capabilities in Programs Including Information Technology," March 3, 2022, as amended

Director of National Intelligence Memorandum ES 2017-00043, "(U) Wireless Technology in the Intelligence Community," January 19, 2017

Director of National Intelligence Memorandum, "Reciprocal Use of Secure Facilities for Controlled Access Program and Special Access Program Discussions," November 30, 2023[3]

Director, Special Access Program Central Office, "DoD Joint Special Access Program (SAP) Implementation Guide (JSIG)," April 11, 2016[4]

DoD 5010.12-M, "Procedures for the Acquisition and Management of Technical Data," May 14, 1993, as amended

DoD Chief Information Officer Memorandum, "Department of Defense Standards and Reciprocity of Special Access Programs Information Technology Devices," April 20, 2020[5]

DoD Directive 2060.01, "Implementation of, and Compliance with, Arms Control Agreements," June 23, 2020

DoD Directive 5000.01, "The Defense Acquisition System," September 9, 2020, as amended

DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020

[1] All CNSS documents are available at https://www.cnss.gov/cnss
[2] Available at https://www.milsuite.mil/book/groups/dodissuances/pages/memos-and-security-policy-memos
[3] Copies of ODNI memorandums can be requested from ODNI.
[4] Contact your CA SAPCO for a copy.
[5] Copies of this memorandum may be requested from the Office of the DoD CIO.

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5200.47E, "Anti-Tamper (AT)," September 4, 2015, as amended

DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended

DoD Directive 5205.07, "Special Access Program Policy," September 12, 2024

DoD Directive 5210.50, "Management of Serious Security Incidents Involving Classified Information," October 27, 2014, as amended

DoD Directive 5230.20, "Visits and Assignments of Foreign Nationals," June 22, 2005

DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended

DoD Directive 5240.06, "Counterintelligence Awareness and Reporting (CIAR)," May 17, 2011, as amended

DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," April 5, 2019

DoD Instruction 2040.02, "International Transfers of Technology, Articles, and Services," March 27, 2014, as amended

DoD Instruction 3305.13, "DoD Security Education, Training, and Certification," February 13, 2014, as amended

DoD Instruction 5000.82, "Requirements for the Acquisition of Digital Capabilities," June 1, 2023

DoD Instruction 5000.83, "Technology and Program Protection to Maintain Technological Advantage," July 20, 2020, as amended

DoD Instruction 5010.44, "Intellectual Property (IP) Acquisition and Licensing," October 16, 2019

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5200.02, "DoD Personnel vetting Program (PSP)," March 21, 2014, as amended

DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015, as amended

DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)," March 6. 2020

DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs," September 12, 2024

DoD Instruction 5205.16, "The DoD Insider Threat Program," December 20, 2024

DoD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures," August 12, 2010, as amended

DoD Instruction 5220.31, "National Industrial Security Program," May 9, 2023

DoD Instruction 5230.09, "Clearance of DoD Information for Public Release," January 25, 2019, as amended

DoD Instruction 5230.29, "Security and Policy Review of DoD Information for Public Release," August 13, 2014, as amended

DoD Instruction 5240.05, "Technical Surveillance Countermeasures (TSCM)," April 3, 2014, as amended

DoD Instruction O-5240.10, "Counterintelligence (CI) in the DoD Components," April 27, 2020

DoD Instruction O-5240.24, "Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)," June 8, 2011, as amended

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

DoD Instruction 5535.08, "DoD Domestic Technology Transfer Program," September 22, 2022

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

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

DoD Manual 5105.21, Volume 3, "Sensitive Compartmented Information (SCI) Administrative Security Manual: Administration of Personnel Security, Industrial Security, and Special Activities," October 19, 2012, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5200.02, "Procedures for the DoD Personnel Vetting Program (PSP)," April 3, 2017, as amended

DoD Manual 5200.08, Volume 3, "Physical Security Program: Access to DoD Installations," January 2, 2019, as amended

DoD Manual 5200.45, "Original Classification Authority and Writing a Security Classification Guide," January 17, 2025

DoD Manual 5220.32, Volume 1, "National Industrial Security Program: Industrial Security Procedures for Government Activities," August 1, 2018, as amended

DoD Manual 8140.03, "Cyberspace Workforce Qualification and Management Program," February 15, 2023

DoD Manual 8180.01, "Information Technology Planning for Electronic Records Management," August 4, 2023

Executive Order 12968, "Access to Classified Information," August 2, 1995

Executive Order 13526, "Classified National Security Information," December 29, 2009

Executive Order 13556, "Controlled Unclassified Information," November 4, 2010

Federal Specification FF-L 2740B, "Locks, Combination, Electromechanical," June 15, 2011[6]

[6] Available at https://fedspecs.gsa.gov/s/federal-specifications

Homeland Security Presidential Directive 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004[7]

Intelligence Community Directive 124, "Electronic Medical Devices," April 26, 2024[8]

Intelligence Community Directive 503, "Intelligence Community Information Environment Risk Management," October 25, 2024

Intelligence Community Directive 703, "Protection of Classified National Intelligence, Including Sensitive Compartmented Information," June 21, 2013

Intelligence Community Directive 705, "Sensitive Compartmented Information Facilities," May 26, 2010

Intelligence Community Policy Guidance 704.5, "Intelligence Community Personnel Security Database Scattered Castles," February 25, 2020[9]

National Counterintelligence and Security Center, "Technical Specifications for Construction and Management of Sensitive Compartmented Information Facilities," current edition (referred to in this issuance as the "NCSC SCIF Specifications")

National Institute of Standards and Technology, "Risk Management Framework," current edition

National Security Agency/Central Security Service Policy Manual 9-12, "Storage Device Sanitization and Destruction Manual," December 4, 2020

National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990[10]

National Security Memorandum 8, "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," January 19, 2022[11]

Office of Management and Budget Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," December 12, 2005[12]

Office of the Secretary of Defense Memorandum, "Renewed Business Rules and Templates for Correspondence and Read Aheads," October 22, 2021[13]

Office of the Secretary of Defense Records Disposition Schedule, current edition

Acting Under Secretary of Defense for Intelligence and Security Memorandum, "DoD Security Review Follow-on Actions: Top Secret Accountability and Managing Access to Classified Information of DoD Systems and Networks," April 16, 2024[14]

Under Secretary of Defense for Intelligence and Security Memorandum, "Implementation of Security Executive Agent Directive 3, Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position," November 2, 2020[14]

United States Code, Title 5

---

[7] Available at https://www.dhs.gov/homeland-security-presidential-directive-12

[8] Intelligence Community Directives are available at https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives

[9] Intelligence Community Policy Guidance documents are available at https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-policy-guidance

[10] Available at https://www.nsa.gov/Culture/Operating-Authorities/

[11] Available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/

[12] Contact the Office of Management and Budget for a copy of the memorandum.

[13] Available at https://www.milsuite.mil/book/groups/dodissuances/pages/memos-and-security-policy-memos

[14] Copies of this memorandum may be requested from the OUSD(I&S).

United States Code, Title 10, Section 119
United States Code, Title 40, Chapter 113
United States Code, Title 42
United States Code, Title 44