DoD Instruction 5205.11

Management, Administration, and Oversight of DoD Special Access Programs

Originating Component:	Office of the Performance Improvement Officer and Director of Administration and Management
Effective:	September 12, 2024
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs," February 6, 2013, as amended
Incorporates and Cancels:	Deputy Secretary of Defense Memorandum, "Interim Integrated Joint Special Technical Operations (IJSTO) Policy," April 5, 2021
Incorporates:	Attachments 2, 3, and 5 of Deputy Secretary of Defense Memorandum, "Implementation Guidance for DoD Special Access Program Enterprise Reform," July 11, 2023
Approved by:	Kathleen H. Hicks, Deputy Secretary of Defense

Purpose: This issuance establishes policy, assigns responsibilities, and prescribes procedures for the management, administration, and oversight of all DoD special access programs (SAPs) in accordance with Executive Order (E.O.) 13526 and DoD Directive (DoDD) 5205.07.

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 (CJCS) and the Joint Staff (JS), the Combatant Commands (CCMD), 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. DoD Component contractors and consultants who require access to DoD SAPs pursuant to the terms and conditions of a contract or agreement.

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

1.2. POLICY.

a. DoD establishes SAP umbrellas at tier 1 of the SAP architecture. Umbrellas will contain SAP compartments at tier 2 and SAP sub-compartments at tier 3 and below, organized to group similar capabilities or information into a single compartment or sub-compartment. Similar critical program information (CPI) will be grouped into a single SAP. Each program at every tier of the architecture is considered an individual SAP.

b. Only the Secretary of Defense or Deputy Secretary of Defense may alter the structure of the enduring SAP architecture at tier 1, including establishment and disestablishment of SAP umbrellas. The Director, DoD Special Access Program Central Office (SAPCO) may approve establishment and disestablishment of DoD SAPs at tiers 2 and below. The Deputy Secretary of Defense approves establishment of SAPs to protect new and novel CPI at all tiers of the SAP architecture.

c. There are two types of SAPs in the SAP architecture: Structural SAPs that provide organization to the architecture and do not protect distinct CPI; and content SAPs that protect distinct CPI.

d. CPI will be protected at the lowest possible tier of the architecture. Structural SAPs may have subordinate sub-compartments. Content SAPs will not have subordinate sub-compartments beneath them.

e. DoD SAP management will account for protection of CPI through the complete lifecycle of the associated capability or information from the time of its identification, through development and potential deployment, if applicable, including collaboration with interagency partners and foreign governments.

(1) The DoD SAP Enterprise will give appropriate attention to each element of SAP lifecycle management: establishment, management, administration, inclusion, apportionment, sharing, and disestablishment.

(2) Lifecycle planning will include criteria for disestablishment of SAP compartments and sub-compartments, or transfer of CPI to collateral security protections, when SAP security protection and controls are no longer necessary based on an analysis of risks and warfighter needs.

f. The Secretary of Defense may designate select unacknowledged SAPs as "waived" when it is determined that using standard procedures for reporting to Congress would adversely affect national security, pursuant to Section 119 of Title 10, United States Code. Waived SAPs remain subject to congressional oversight.

g. DoD will share DoD SAP-protected information to the greatest extent practicable with foreign governments who have capabilities, platforms, and operations that complement U.S. warfighting priorities, consistent with existing authorities and processes for defense partnerships and information sharing with foreign governments.

h. Disclosure of DoD SAP-protected information and participation in SAPs with other U.S. Government agencies and foreign governments will be approved by the Secretary of Defense or Deputy Secretary of Defense, unless otherwise delegated.

i. Defense Counterintelligence and Security Agency (DCSA) oversight for the administration of the National Industrial Security Program will be phased out in July 2029 in accordance with the carve-out provision of DoD Instruction (DoDI) 5220.31.

SECTION 2: RESPONSIBILITIES

2.1. PRINCIPAL STAFF ASSISTANTS (PSAS) DESIGNATED AS SAP OVERSIGHT AUTHORITIES (OAS).

As DoD SAP OAs, the Under Secretary of Defense for Research and Engineering (USD(R&E)), Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), Under Secretary of Defense for Policy (USD(P)), and the Under Secretary of Defense for Intelligence and Security (USD(I&S)):

a. Perform the responsibilities described in Paragraphs 3.1. and 3.3.

b. Establish and maintain a SAPCO and designate a SAPCO director to oversee SAPs for which the OA has responsibility.

2.2. DIRECTOR, DOD SAPCO.

As a DoD SAP OA under the authority, direction, and control of the Deputy Secretary of Defense, the Director, DoD SAPCO performs the responsibilities described in Paragraphs 3.1. and 3.3.

2.3. PSAS AND DOD COMPONENT HEADS DESIGNATED AS SAP COGNIZANT AUTHORITIES (CAS).

The PSAs and DoD Component heads designated as SAP CAs by the Secretary of Defense or the Deputy Secretary of Defense:

a. Perform the responsibilities described in Paragraphs 3.2. and 3.3.

b. Establish and maintain a SAPCO and designate a SAPCO director to be responsible for managing the use of SAP protection for capabilities and information for which the PSA or DoD Component head has responsibility. The Secretaries of the Navy and Air Force may establish an additional SAPCO and designate an additional SAPCO director for the Marine Corps and Space Force, respectively.

2.4. USD(R&E).

In addition to the responsibilities in Paragraphs 2.1. and 2.3., the USD(R&E) identifies and cultivates cutting-edge technology development, technology transition, developmental prototyping, experimentation, and developmental testing activities and programs requiring SAP protection to ensure continued U.S. warfighting advantage.

2.5. USD(A&S).

In addition to the responsibilities in Paragraphs 2.1. and 2.3., the USD(A&S):

a. Provides support for special access defense acquisition boards, in-progress reviews, integrated acquisition portfolio reviews, and other OSD-led acquisition forums.

b. Participates in DoD efforts to resolve technology protection, technology transfer, and technology export issues.

c. Provides support for SAP-level Committee on Foreign Investment in the United States tasks pursuant to E.O. 11858 and the foreign ownership, control, and influence certification process.

2.6. USD(P).

In addition to the responsibilities in Paragraphs 2.1. and 2.3., the USD(P):

a. Provides management and oversight to the OSD special technical operations cell, which addresses required SAP-related actions between OSD and the integrated joint special technical operations (IJSTO) process in coordination with the DoD SAPCO.

b. Ensures foreign government participation in DoD SAPs and the foreign disclosure of SAP information is consistent with National Disclosure Policy-1 and the National Defense Strategy.

2.7. USD(I&S).

In addition to the responsibilities in Paragraphs 2.1. and 2.3., the USD(I&S):

a. Oversees preparation and submittal of DoD intelligence SAP reports to the congressional intelligence committees as required by law.

b. Serves as the primary interface for the Director of National Intelligence's (DNI) Controlled Access Program Central Office for all relevant issues, pursuant to Intelligence Community Directive 906. This includes all issues related to Intelligence Community (IC) compartmented capabilities or information proposed or approved for inclusion.

c. Serves as the SAPCO for the Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency.

d. In coordination with the DNI's Controlled Access Program Central Office, deconflicts the names and abbreviations for DoD SAPs and the DNI's controlled access programs.

2.8. CJCS.

In addition to the responsibilities in Paragraph 2.3., the CJCS:

a. Serves as the only entry point for any DoD SAPs into the JS and CCMDs. Any organization or program office, to include non-DoD agencies, that wants to access JS and CCMD personnel to a program must coordinate the program access request (PAR), as described in Paragraph 5.2.f., with the JS SAPCO before conducting a SAP indoctrination.

b. Accredits all JS and CCMD SAP facilities (SAPFs) and authorizes information systems, unless delegated to the CCMD SAP control (SAPCON) officer or SAP security manager.

2.9. COMBATANT COMMANDERS (CCDRs).

The CCDRs:

a. Appoint a SAPCON Officer to coordinate and oversee any SAP activity within the command.

b. Perform all CCMD responsibilities in Section 6.

SECTION 3: SAP PROCEDURES

3.1. OFFICIALS DESIGNATED AS AN OA.

The PSAs and DoD Component heads designated as SAP OAs:

a. Oversee SAPs for which the OA has been assigned authority.

b. Ensure the work done within a SAP is within the approved program scope.

c. Conduct an annual review of all DoD SAPs regarding continuation of SAP security protection in accordance with E.O. 13526 and DoDD 5205.07. Provide recommendations to the Senior Review Group (SRG), established by DoDD 5205.07, for Special Access Program Oversight Committee (SAPOC) approval.

d. Endorse inclusion, apportionment, or deapportionment of SAPs for CCMD use through the IJSTO process.

e. Ensure SAPs do not duplicate or overlap.

f. Provide input to and coordinate on SAP reports to Congress, as required.

g. Coordinate with all other OAs on oversight of SAPs for which the OA is also the CA.

3.2. OFFICIALS DESIGNATED AS A CA.

The PSAs and DoD Component heads designated as CAs over SAPs:

a. Initiate SAP life cycle management actions, as required, in accordance with Section 4.

b. Contribute to annual SAP Enterprise reviews of all SAPs in which the CA is a stakeholder to validate that the associated CPI still needs SAP protections. If a SAP has multiple stakeholders, the stakeholders collaborate to jointly validate that the CPI continues to need SAP protections.

c. Provide security classification guide (SCG) annexes to the DoD SAPCO for each SAP in which the DoD Component is a stakeholder, in accordance with Paragraph 5.3.

d. Serve as the office of primary responsibility (OPR) for SAPs for which the CA initiated establishment, unless all stakeholders agree to designate a different stakeholder as OPR. SAP OPRs lead CA collaboration on developing SCG annexes and contributing to annual SAP Enterprise reviews for SAPs in which there are multiple stakeholders.

e. Support the Director, DoD SAPCO and the SAP governance structure in reporting the state of DoD SAPs to congressional committees, in accordance with congressional reporting requirements.

f. Ensure that SAP-protected capabilities are properly evaluated for potential critical assets in accordance with Defense Critical Infrastructure Program policy guidance outlined in DoDD 3020.40.

g. Appoint authorizing officials for SAP information systems and accrediting officials for SAPFs. If the authorizing officials or accrediting officials are outside of the DoD Component SAPCO, the officials coordinate the authorization and accreditation decisions with the DoD Component SAPCO.

h. Provide comprehensive counterintelligence (CI) support to DoD SAPs in accordance with DoDD 5240.02 using organic or servicing CI organizations.

i. Conduct Planning, Programming, Budgeting, and Execution authorities for their respective capabilities and information protected by DoD SAPs, as described in applicable DoD policies and issuances.

j. All DoD Components using DCSA for industrial security oversight will designate a cognizant security office other than DCSA to perform this function and will complete all associated actions by July 2029. DoD Component-designated industrial security oversight procedures will, at a minimum, meet the standards and frequency authorized by Part 117 of Title 32, Code of Federal Regulations, also known as the "National Industrial Security Program Operating Manual."

3.3. OFFICIALS DESIGNATED AS OA OR CA.

In addition to the responsibilities in Paragraphs 2.1., 2.2., 2.3., 3.1., and 3.2., PSAs and DoD Components heads with OA or CA over SAPs:

a. Provide support to the Director, DoD SAPCO for congressional meetings. Coordinate and prepare responses to congressional SAP inquiries through the Director, DoD SAPCO.

b. Oversee and maintain a dedicated cadre to administer and execute SAP security, audit, compliance, and cybersecurity activities for assigned SAPs.

c. Determine whether to employ random CI scope and issue-based polygraph and credibility assessments for SAP-accessed personnel for which they are responsible, in accordance with DoDI 5210.91.

d. Propose realignment of CPI within the SAP architecture, where necessary.

e. Ensure all records and information related to DoD SAPs are retained in accordance with the DoD Component records management policies, procedures, and disposition authorities as approved by the National Archives and Records Administration pursuant to:

(1) Chapters 29, 31, and 33 of Title 44, United States Code.

(2) Parts 1220-1228 of Title 36, Code of Federal Regulations.

(3) DoDI 5015.02.

(4) DoD Manual (DoDM) 8180.01.

f. Support and execute individual DoD Component and team inspections in accordance with guidance that the Director, DoD SAPCO publishes.

g. Assess new SAPs upon establishment for future releasability to foreign governments. Via the Director, DoD SAPCO, coordinate participation by foreign governments in joint SAPs and sharing of SAP-protected capabilities and information. DoD cooperation with foreign governments on SAP-protected capabilities and information will be governed by existing and future agreements that establish the relationship of the participants regarding security, administration, decision making, resourcing, and other associated matters, consistent with DoDI 5530.03.

3.4. SAPCO DIRECTORS.

Under the authority, direction, and control of an OA or CA, the SAPCO directors:

a. Implement policies and procedures for the execution, management, administration, security, and records management of SAP protections that the respective OA or CA oversees or uses.

b. Submit proposed SAP governance actions to the Director, DoD SAPCO through the OA or CA's member of the SAP Senior Working Group (SSWG), established by DoDD 5205.07, for subsequent SSWG review, in accordance with Sections 3 and 4 of this issuance.

c. Exercise administrative control of component SAP activities, including decisions on access eligibility of CA personnel.

d. Nominate SAP-protected capabilities and information for inclusion and subsequent apportionment to CCMDs in accordance with the IJSTO process and procedures outlined in Paragraph 6.3.

e. Coordinate MOAs and memorandums of understanding (MOUs) for cooperation on SAP-protected DoD activities with other U.S. Government agencies following Secretary of Defense or Deputy Secretary of Defense approval for disclosure of the relevant SAP-protected information, in accordance with DoDI 4000.19. The CA SAPCO director submits MOAs and MOUs with interagency partners for SSWG review via the CA's SSWG member before CA approval.

f. Facilitate international agreements for foreign government involvement with DoD SAPs.

3.5. SAP GOVERNANCE BODIES.

a. SAPOC.

The SAPOC, established by DoDD 5205.07, convenes at the direction of the Deputy Secretary of Defense to:

(1) Review issues referred by the SRG.

(2) Ensure the warfighting capability needs of the CCMDs and the requirement for an integrated joint force (JF) are reflected in life-cycle management considerations for all DoD SAPs.

(3) Conduct an annual review of DoD SAPs to assess the continuing need for protection of CPI within SAP security controls, in accordance with E.O. 13526 and DoDD 5205.07. In the annual review, the SAPOC will also assess:

(a) Readiness for apportionment of SAP capabilities through the IJSTO process.

(b) SAP sharing with interagency partners and foreign governments.

(c) Potential for SAP disestablishment when additional protection methods are no longer warranted.

(d) All waived DoD SAPs to determine the need for continued waived status.

b. SRG.

(1) The SRG provides a forum for senior DoD leaders to provide recommendations to higher leadership; identify and adjudicate issues; resolve conflicts and constraints; and ensure alignment of SAP protections.

(2) The SRG convenes at the direction of the Deputy Secretary of Defense or the recommendation of the Director, DoD SAPCO to:

(a) Resolve or refer to the SAPOC SAP-related issues.

(b) Provide recommendations to the Deputy Secretary of Defense and SAPOC regarding SAP management, administration, and oversight for programs submitted for SRG review.

(c) Provide recommendations to the SAPOC and Deputy's Management Action Group regarding the utility of DoD SAPs in support of DoD capability needs and the requirement for an integrated JF pursuant to DoDD 5105.79.

c. SSWG.

The SSWG:

(1) Reviews and provides recommendations on proposed SAP governance actions.

(2) Addresses the transition of SAP capabilities to apportioned access to support joint warfighting integration.

(3) Conducts periodic reviews of SAP management and execution to inform SRG and SAPOC oversight.

(4) Enables collaboration with the U.S. interagency, foreign governments, and industry with respect to DoD SAPs.

(5) Shares information to ensure horizontal protection of similar capabilities and information and to capture best practices across the DoD Components for all DoD SAPs.

(6) Reviews emerging technologies and new capabilities for potential special access protection.

(7) Approves DoD SAPs and DoD SAP CPI for use in SAP studies and portfolios and approves access management structures for studies and portfolios, except as noted in Paragraph 5.2.g.

(8) Establishes and tasks SAP working groups to develop and recommend SAP policy changes, conduct SAP classification reviews, and perform other governance duties as assigned.

3.6. SAP GOVERNANCE.

a. The SAP governance bodies, as established in DoDD 5205.07, review and provide recommendations regarding proposed SAP governance actions, including but not limited to:

(1) Requests to establish SAP security protections for newly identified CPI. SAP governance bodies determine whether the new CPI is novel or can be properly included within existing SAP security protections.

(2) Determination of type and classification of new SAPs.

(3) Proposals to disestablish a DoD SAP umbrella, compartment, or sub-compartment.

(4) Designation of, and changes to, CA.

(5) Inclusion, apportionment, and deapportionment of SAPs to and from CCMDs via the IJSTO process.

(6) Alteration of an existing SAP's scope or type.

(7) Use of DoD resources to support DoD and non-DoD SAPs, except for those approved in accordance with the provisions of DoDD S-5210.36.

(8) Foreign government access to and participation in DoD SAPs.

b. CA SAPCOs will submit proposed SAP governance actions to the Director, DoD SAPCO through the DoD Component's SSWG member.

(1) Upon notification, the Director, DoD SAPCO will inform the SSWG membership of the proposed actions.

(2) The Director, DoD SAPCO will schedule reviews with the SSWG, SRG, and SAPOC as necessary.

(3) Issues on which there is disagreement will be referred to the next higher governance body for consideration.

c. Once the SAP governance bodies have completed their review of proposed SAP governance actions and reached agreement on a recommendation, the Director, DoD SAPCO will forward the recommendation to the Deputy Secretary of Defense for approval or disapproval, with the exceptions noted in Paragraphs 3.6.c.(1)-(3). Recommendations will include any alternative views of dissenting members.

(1) The Director, DoD SAPCO, with SSWG concurrence, may approve SAP establishment and disestablishment, including designation of and changes to SAP type, scope, and classification, at tiers 2 and below of the SAP architecture. The Deputy Secretary of Defense approves establishment of SAPs to protect new and novel CPI at all tiers of the SAP architecture.

(2) The Director, DoD SAPCO, with SSWG concurrence, may approve SAP protection for sensitive capabilities and information and placement into the existing architecture. Addition of new capabilities or information into the existing SAP architecture does not necessarily constitute a scope change that requires Deputy Secretary of Defense approval, but may drive other changes, such as SCG updates.

(3) CAs may disestablish capabilities or information from SAP protection when the SAP providing protection is left intact within the architecture. CAs will follow the procedures described in Paragraph 4.2.

d. Following Deputy Secretary of Defense decision on a SAP governance action, the Director, DoD SAPCO will provide a copy of the Deputy Secretary of Defense approval or disapproval memorandum to the CA SAPCO and the SSWG.

(1) The DoD SAPCO will notify the congressional defense committees of changes to CPI protected by DoD SAPs and will also notify the congressional intelligence committees of changes to CPI that is designated as intelligence or intelligence related.

(2) The DoD SAPCO will notify the appropriate members of congressional defense committees (and the intelligence committees for an intelligence or intelligence-related SAP) once a decision has been made to change the classification of a DoD SAP or to declassify a DoD SAP and make it public. The DoD SAPCO will submit a report to the appropriate congressional defense committees (and the intelligence committees for an intelligence or intelligence-related SAP) containing a description of the proposed change(s), the reasons for the change(s), and notice of any public announcement planned to be made with respect to the proposed change(s).

e. CAs will maintain all SAP personnel access and SAPF documentation in a single, authoritative repository defined by the Director, DoD SAPCO in coordination with the DoD Chief Information Officer. All workflow activity for these purposes will occur in this repository for universal awareness across the DoD SAP Enterprise.

SECTION 4: LIFE-CYCLE MANAGEMENT

4.1. SAP ESTABLISHMENT.

The addition of new umbrellas or compartments in the SAP architecture will be rare. To the extent possible, CPI for new capabilities or information requiring SAP protection will be incorporated into existing SAPs containing similar CPI.

a. Newly Identified CPI.

Proposals to provide SAP protections to newly identified CPI will use the Transitional Repository (TR) umbrella, following this process:

(1) The initiating CA will submit a request to DoD SAPCO to create a SAP project. DoD SAPCO will create the project in the TR umbrella and assign a unique project number, unless the Director, DoD SAPCO approves an exception. The DoD SAPCO will make available a template for SAP project requests.

(2) Within 45 calendar days of creation of the SAP project, the CA will submit to DoD SAPCO a plan to place the CPI into the SAP architecture. CA principal written endorsement of the plan is required if the initiating CA recommends creating a new SAP umbrella or compartment or requests a waiver for a SAP project to exceed 210 calendar days.

(3) The project plan will include, at a minimum:

(a) Plain language description of the CPI requiring SAP protection.

(b) Explanation of why collateral security controls are insufficient to protect the CPI.

(c) Proposed SAP type (acknowledged or unacknowledged).

(d) Highest level of classification of the CPI.

(e) CA assessment of where the project should be placed in the SAP architecture, or justification to create a new umbrella, compartment, or sub-compartment in the SAP architecture.

(f) Conditions for inclusion, eventual apportionment, and releasability.

(g) Criteria for disestablishment.

(h) SCG annex. The draft SCG annex will be developed in accordance with DoDM 5200.45. It will include statements describing the expected effect the SAP capability will provide to the warfighter at the collateral and special access levels. Programs that are unable to provide effects-based statements at collateral levels may list “not releasable at this level” in this section of the SCG annex.

(i) Recommendation on whether the CPI should be shared with foreign governments.

(4) The Director, DoD SAPCO will convene the SSWG to assess the plan and placement of the newly identified CPI into the enduring SAP architecture.

(5) Creation of a SAP project will result in one of the following outcomes:

(a) Addition to an existing SAP within the enduring architecture. With SSWG concurrence, the Director, DoD SAPCO may add new capabilities or information under the protections of an existing SAP in the architecture.

(b) Establishment of a new SAP. If the SSWG determines the proposed newly identified CPI requires a new SAP umbrella or is new and novel, the Director, DoD SAPCO will submit the establishment recommendation to the Deputy Secretary of Defense for decision. The Director, DoD SAPCO may approve the establishment of new SAP compartments and sub-compartments not protecting new and novel CPI.

(c) Termination of the project if the SSWG determines the CPI does not meet the criteria for SAP protections described in E.O. 13526, or any successor E.O.s, and DoDD 5205.07. SAP projects will be automatically transferred to the appropriate TR sub-compartment for termination if a decision is not reached within 210 calendar days without a waiver. Only the Secretary of Defense or Deputy Secretary of Defense may approve waivers for SAP projects creating a new SAP umbrella to exceed 210 calendar days.

(6) A new SAP umbrella may not be created until the Director, DoD SAPCO has notified the congressional defense committees in writing and 30 calendar days have passed after delivery of the notification.

b. SAP Management Over the Life Cycle of a Capability.

(1) Proposals to establish SAP protection for CPI associated with an existing SAP-protected capability as the capability evolves through its life cycle from research and development through acquisitions and operational fielding will use the TR umbrella.

(2) CAs, through the Director, DoD SAPCO, will propose to the SSWG protection of CPI associated with a capability currently under SAP protections when that capability reaches the appropriate stages in its life cycle. The proposal will include:

(a) Plain language description of the existing capability's progress through its life cycle and the related CPI.

(b) Review of the existing CPI characteristics (acknowledged or unacknowledged; highest level of classification; and conditions for inclusion, eventual apportionment, and releasability) and recommendations on characteristics for the new, associated CPI.

(c) CA assessment of where the new, associated CPI should be placed in the SAP architecture or justification for creation of a new umbrella, compartment, or sub-compartment in the SAP architecture.

(d) Required SCG annex updates, if any.

(e) Criteria for disestablishment.

(f) Recommendation on whether the CPI should be shared with foreign governments.

(3) DoD SAPCO will assign a SAP project number for the CPI, unless the Director, DoD SAPCO approves an exception.

(4) The Director, DoD SAPCO will convene the SSWG to assess the proposal and decide on placement of the CPI into the SAP architecture.

(5) Inclusion is an essential part of SAP life cycle management that enables apportionment via the IJSTO process. Inclusion is a unique event in the life cycle of a capability and will be accomplished in accordance with the procedures described in Paragraph 6.3.a.

c. Transition of CPI to a Different SAP.

If it is determined that CPI for specific capabilities or information would be more appropriately protected under a different SAP, the CA may propose to the SSWG to transition the CPI within the SAP architecture. The proposal will include:

(1) Explanation of why the capability should be protected under a different SAP and assessment of where it should be placed in the SAP architecture.

(2) Review of and recommendations on CPI characteristics (acknowledged or unacknowledged; highest level of classification; and conditions for inclusion, apportionment, and releasability). Changes of type or classification of SAP umbrellas require Deputy Secretary of Defense approval.

(3) Required SCG annex updates, if any.

(4) Impacts to interagency collaboration.

(5) Impacts to foreign relations.

(6) Criteria for disestablishment.

(7) Impact to inclusion or apportionment.

4.2. SAP DISESTABLISHMENT.

a. The removal of umbrellas or compartments from the SAP architecture will be rare. Disestablishment actions will most often be associated with individual capabilities or information, rather than umbrellas, compartments, or sub-compartments, thereby leaving the umbrella, compartment, or sub-compartment intact within the SAP architecture.

b. A CA that proposes to disestablish a SAP umbrella, compartment, or sub-compartment, or to disestablish SAP protection for a capability or information within an enduring compartment or sub-compartment, will submit a disestablishment proposal to the SSWG for concurrence. Upon SSWG concurrence, the Director, DoD SAPCO may approve disestablishment of SAP compartments and sub-compartments. Proposals to disestablish SAP umbrellas will be submitted to the Deputy Secretary of Defense for approval. The DoD SAPCO will prepare an action memorandum for Deputy Secretary of Defense approval of disestablishment actions, as necessary, and will prepare Deputy Secretary of Defense letters notifying Congress of the disestablishment(s).

c. Once disestablishment is approved and congressional notification, if required, is complete, the SAP umbrella, compartment, or sub-compartment and its associated program identifier will be in "closeout." Steps to remove inheritances, accesses, and other dependencies will be taken as part of the disestablishment process. SAP security protection will be retained until all the required disestablishment actions are complete and the SAP is officially disestablished.

d. CAs will document actions required to execute approved disestablishment proposals in a disestablishment plan and will share the disestablishment plan with the SSWG for awareness. If the SAP umbrella, compartment, or sub-compartment being disestablished protects CPI associated with more than one capability or set of information, a disestablishment plan must be developed and shared for each capability or set of information. Disestablishment plans will address, at a minimum:

(1) Information security, operations security, personnel security, physical security, industrial security, cybersecurity, and communications security processes applicable during and after disestablishment.

(2) Administrative actions, including contracting, fiscal, audit, property disposition, classified material disposition, training, public affairs, legal, logistics, and technical actions.

(3) Deapportionment, in accordance with Section 6.

(4) Impacts on cooperation with interagency partners and foreign governments.

(5) Impacts on other DoD SAPs.

(6) Required SCG addendum updates, if any.

(7) Final disposition of the CPI after disestablishment is complete in accordance with Paragraph 4.2.e.

e. There are two potential outcomes for final disposition of SAPs being disestablished:

(1) Archive.

Archived SAPs will retain their former SAP security protections. All inheritances and other dependencies will be terminated. Only the stakeholder SAPCOs, OA SAPCOs, and the

DoD SAPCO will retain access to archived SAPs and may approve additional accesses as necessary to inform current activities.

(2) Termination.

Termination occurs when the CPI has been transitioned to collateral protections or other SAP security protections, or there is no CPI to archive, transition, or declassify.

SECTION 5: SECURITY

5.1. SAP ACCESS PREREQUISITES.

DoD Components will consider suitability and loyalty to further control SAP access to meet E.O. 13526 requirements for enhanced security. The sensitivity of the information dictates additional safeguards as approved by the Secretary of Defense or Deputy Secretary of Defense. To be accessed to a DoD SAP, the candidate must:

a. Be formally nominated for access by a person currently accessed to the same DoD SAP who can make a need to know (NTK) and contribution recommendation to the access approval authority (AAA). In their assessment of NTK, AAAs will consider an individual's potential to facilitate collaboration and innovation across separate but related programs for access to Joint Force Integration SAPs. An individual's potential to facilitate collaboration and innovation will not be considered when determining access to Strategic Enabler SAPs.

b. Have a current SECRET or TOP SECRET clearance, as appropriate for the program(s) being accessed, based upon established investigative standards for access to SECRET and TOP SECRET information. Accessing personnel holding an INTERIM SECRET or INTERIM TOP SECRET clearance is authorized on a case-by-case basis and must be approved by an OA or the CA SAPCO, in coordination with other stakeholders for the SAP(s) being accessed.

c. Have an acceptable investigation or have been enrolled in continuous evaluation or continuous vetting.

d. Meet SAP eligibility requirements in accordance with the SAP nomination process as described in Volume 2 of DoDM 5205.07, or a successor issuance.

e. Be subject to a random CI-scope polygraph examination.

(1) The use of a polygraph examination as a mandatory access determination requirement must be approved by the Secretary of Defense or Deputy Secretary of Defense and be consistently applied to all candidates, in accordance with DoDI 5210.91.

(2) CI-scope polygraph examinations must not be used as the only basis for granting access to DoD SAPs. Exceptions to these requirements will only be granted by the Secretary of Defense or Deputy Secretary of Defense.

(3) Specific polygraph examinations to resolve issues related to SAP access eligibility will be administered in accordance with DoDI 5210.91.

(4) CI polygraph examinations are considered current when administered within the past 5 years, although more stringent requirements may be established.

f. Sign a DoD-approved SAP program indoctrination and non-disclosure agreement.

5.2. ACCESS MANAGEMENT.

a. CAs and OAs will designate individuals as AAAs to approve component personnel for access to DoD SAPs for which the CA or OA has SAP management or oversight responsibilities. AAAs may grant SAP access to personnel who meet all access prerequisites.

b. Personnel with access to a DoD SAP will inherit access to its subordinate SAP elements, unless explicitly excepted by the Director, DoD SAPCO.

c. Access management and procedures differ between Joint Force Integration SAPs and Strategic Enabler SAPs. CAs have AAA for all SAPs in which the CA is a stakeholder, including SAPs that have multiple stakeholders.

(1) AAA for SAP-protected information within Joint Force Integration SAP umbrellas may be delegated by CAs to the lowest practical echelon within each DoD Component.

(2) AAA for information within Strategic Enabler SAP umbrellas will be managed by the CA's DoD Component head and may not be delegated below the DoD Component's CA SAPCO staff or the SAP program manager.

d. Table 1 identifies the appropriate AAA for access approval. AAAs will coordinate with their DoD Component's SAPCO director to verify the intended SAP-protected information is contained within a SAP designated for use by the DoD Component. Detailed procedures for SAP access are in Volume 2 of DoDM 5205.07, or a successor issuance.

e. A currently accessed person will submit a PAR to a designated official for individuals assessed to have NTK. The designated official will review and submit the PAR for additional review, as required, and approval by the appropriate AAA. Any DoD Component desiring to access another DoD Component's personnel to a SAP must coordinate the PAR with the other DoD Component's SAPCO.

f. PARs will be submitted via the authoritative SAP repository. In the absence of access to the repository, the currently accessed person will coordinate with the DoD Component's SAPCO to submit the PAR. The DoD Component's SAPCO will coordinate the PAR, as required, via the authoritative SAP repository.

g. The Director, DoD SAPCO will annually request Deputy Secretary of Defense approval of the access management structure that assigns individuals access to the entire suite of DoD SAPs based on organization and duty position. The Director, DoD SAPCO is the AAA for individuals in this access management structure.

h. In coordination with the OA SAPCO directors, the Director, DoD SAPCO will make portfolio designations that provide access to a significant number of programs.

Table 1. AAAs

SAP-protected information	Component or position of the individual[1] to be accessed	AAA and procedures[2, 3]
SAP information protected within a Joint Force Integration SAP umbrella	DoD Components Contractors or consultants[4]	AAA may be delegated to lowest practical echelon within the DoD Component. CA and OA SAPCOs are responsible for AAA delegation for their DoD Components.
SAP information protected within a Strategic Enabler SAP umbrella	DoD Components Contractors or consultants[4]	CA or OA SAPCO Director or the SAP program manager.[5]
Any DoD SAP information	Executive, Legislative, or Judicial Branches of the U.S. Government[6, 7]	Approved by Deputy Secretary of Defense or the Director, DoD SAPCO.
Any DoD SAP information	Foreign national	Approved by Deputy Secretary of Defense or the Director, DoD SAPCO.[8] AAA may be delegated by exception.
Foreign government SAP information	All U.S. personnel	Approved by the foreign government or the Director, DoD SAPCO (as delegated by the foreign government).

[1] An "individual" denotes U.S. Government, contractor, and consultant personnel, unless specifically designated as a foreign national.
[2] The Director, DoD SAPCO has AAA for all DoD SAPs unless expressly withheld by the Secretary of Defense or Deputy Secretary of Defense.
[3] JS SAPCO is the servicing CA SAPCO for all JF personnel, with the exception of United States Special Operations Command personnel, whose servicing CA SAPCO is the Assistant Secretary of Defense for Special Operations and Low Intensity Conflict SAPCO.
[4] Contractors and consultants may be granted access to SAP information based on the applicable DD Form 254.
[5] CA and OA SAPCO Directors may delegate AAA for non-waived SAPs to the DoD Component's SAPCO staff. AAA for waived SAPs may be delegated to the SAPCO Deputy Director or alternate designee.
[6] DoD SAPCO will coordinate on PARs for judicial and other federal agency personnel for waived programs.
[7] The Director, DoD SAPCO and the Director, Office of the USD(P) SAPCO will coordinate on PARs for the White House, National Security Council, and political appointees of the Executive Branch. The Director, Office of the USD(I&S) SAPCO will coordinate on PARs for IC elements. The Director, DoD SAPCO, will be informed of accesses for all other personnel from federal agencies by addition to the DoD SAPCO database.
[8] Foreign nationals with citizenships in addition to those of the country of the foreign governments that have nominated them for access to programs already approved for release to those nominating foreign governments requires Secretary of Defense or Deputy Secretary of Defense approval, unless otherwise delegated.

5.3. SCGS.

a. The Director, DoD SAPCO will:

(1) Publish one SCG for each SAP umbrella, in accordance with DoDD 5205.07.

(2) In coordination with the USD(I&S), provide supplemental guidance for the issuance of SAP SCG annexes.

(a) CAs will develop SCG annexes for each SAP within the umbrella in which the CA is a stakeholder. If a SAP has multiple stakeholders, the OPR for the SAP will lead the effort with all stakeholders to draft, sign, and maintain the SCG annex.

(b) SCG annexes will not exceed the scope or broad CPI directed by DoD SAPCO in the corresponding umbrella SCGs.

(c) SCG annexes will be shared with the SSWG for awareness upon issuance or following any updates.

b. All SAP Enterprise SCGs and any supplementary classification guidance will follow guidance issued by the USD(I&S) and will conform and adhere to DoDM 5200.45 unless the USD(I&S) grants an exception to policy.

c. The Director, DoD SAPCO will review SCGs and SCG annexes every 5 years or upon update of the SCG or SCG annex.

5.4. SAP ENTERPRISE-INTELLIGENCE COMMUNITY COLLABORATION.

a. The DoD SAP Enterprise must collaborate with the IC to meet mission requirements and inform national decision making.

b. DoD SAP information will be shared with and available to the IC on appropriately authorized national security information systems in accordance with policy and procedures developed by the DoD Chief Information Officer, in coordination with the Director, DoD SAPCO and in partnership with the Office of the DNI. SAP IT policies and procedures will adhere to requirements established by the National Manager for National Security Systems pursuant to National Security Directive 42 and DoDD 5144.02.

5.5. INDUSTRIAL OVERSIGHT.

a. CAs will designate a cognizant security office other than DCSA to perform industrial security oversight for cleared defense contractor performance on all contracts that require access to DoD SAP information, in accordance with DoDI 5220.31.

b. All new DD Forms 254, "DoD Contract Security Classification Specification," located at https://www.esd.whs.mil/Directives/forms/, for acknowledged DoD SAPs issued after publication of this issuance will be marked "CUI" and processed via the National Industrial Security

Program Classification System, unless the contractor relationship has formalized cover protections in place or as directed by the USD(I&S). A standardized classified addendum will detail all SAP protocols for each contract and may be classified at the SAP level in accordance with applicable SCGs. Classified DD Forms 254 for unacknowledged DoD SAPs will be provided to the appropriate cognizant security office.

c. Industry representatives will be granted access to SAP information for which they are on contract, based on the applicable DD Form 254.

5.6. SAP FACILITY SECURITY.

DoD Components may process all DoD SAP material in any DoD SAPF up to the classification level to which the SAPF is accredited (i.e., SECRET, TOP SECRET) in accordance with the SAPF accreditation letter. A co-utilization agreement may be required when SAP-related activities managed by more than one CA are performed in a single SAPF.

SECTION 6: CJCS AND CCDR PROCEDURES

6.1. GENERAL.

a. Any granting of SAP access to JF (i.e., JS, CCMDs, sub-unified commands, joint functional component commands, joint task forces (JTFs), and the National Guard Bureau) personnel by any organization outside the JF must be coordinated with the JS SAPCO. Additionally, any granting of SAP access to CCMD personnel and personnel assigned to sub-unified commands, joint functional component commands, and JTFs must also be coordinated with the appropriate CCMD SAPCON Office.

b. Access of Service component personnel must be in accordance with Service procedures and coordinated with the owning Military Service or CCMD SAPCON Office. If accessed, the owning Military Service or command SAPCON Office is responsible for annual reviews and SAP refresher training or will coordinate with the CCMD SAPCON Office to provide this support.

6.2. CCMD SAP PROCEDURES.

Each CCMD will have a designated SAPCON Officer who serves as the only entry point for DoD SAPs into the command (after coordination with JS SAPCO). The CCMD SAPCON Officer represents the CCDR and is responsible for coordinating and overseeing any SAP activity within the command, to include sub-unified commands, functional components, and JTFs. Any component, organization, or program desiring to access CCMD personnel (including JTF personnel) to a program must contact the CCMD SAPCON Officer before taking any action to introduce their SAP into the command.

6.3. IJSTO SAP LIFE CYCLE PROCEDURES.

a. Inclusion.

(1) In order to share SAP-protected capabilities and information with CCMDs via the IJSTO process, information relevant to joint planning will be approved for inclusion.

(2) SAP-protected capabilities and information will be approved for inclusion as soon as the capability or information becomes relevant to the CCMD planners. SAP capabilities and information are relevant to the CCMD planners as soon as it is known that a potential operational effect exists or is expected to exist within the next 36 months.

(3) SAP-protected capabilities and information that other U.S. Government agencies and foreign governments share with the DoD via an MOA, MOU, or international agreement may be shared with CCMDs through IJSTO, in accordance with SAP policies and procedures.

(4) CAs will submit requests for inclusion to the Director, DoD SAPCO, who will coordinate with the Office of the USD(P), appropriate OA, and JS SAPCO Directors before approving inclusion.

(5) The SSWG may solicit from CAs an inclusion request regarding SAP-protected capabilities or information that the SSWG assesses may be ready for inclusion and follow-on apportionment.

(6) All SAP-protected capabilities or information approved for inclusion are deemed to be candidates for apportionment and will be submitted for apportionment to CCMDs when appropriate through the IJSTO process unless the Director, DoD SAPCO, in coordination with the USD(P), the appropriate OA, and Vice CJCS, grants a waiver from this requirement.

(7) The CJCS is granted AAA, SAPF accreditation authority, and authority as SAP information system authorizing official for all capabilities and information protected by a DoD SAP upon inclusion, unless the Director, DoD SAPCO has waived the apportionment requirement. The CJCS may further delegate these authorities. For compartmented capabilities or information shared with DoD by another U.S. agency or a foreign government, these authorities will be consistent with the MOA or other agreement made as described in this issuance.

b. Apportionment of SAP-Protected Capabilities and Information.

(1) Operational capabilities and information protected by a SAP and approved for inclusion will be apportioned through the IJSTO process. The IJSTO process grants CCDRs the authority to conduct planning with the capability or information, establishes the authority for deployment and employment of the capability, and confirms the capability complies with all applicable domestic and international law.

(2) CAs will submit to the JS requests to apportion SAP-protected capabilities and information in accordance with procedures established by the CJCS. The request must provide:

(a) Any updates to material provided during inclusion. The documents submitted must include sufficient information to facilitate CCMD planning efforts and contribute to an approved concept of operations.

(b) A written legal review by the applicable DoD Component's legal counsel, which must include a weapons review.

(c) A recommendation on authority levels for approval of deployment and employment with sufficient justification for that recommendation, in accordance with guidance established by the USD(P).

(3) The JS will submit the apportionment request to the Director, DoD SAPCO. The JS will recommend authority levels for deployment and employment and provide sufficient justification for that recommendation in accordance with USD(P) guidance.

(a) The Director, DoD SAPCO will coordinate the request through the SSWG, the SRG, and the SAPOC as required, and submit it to the Deputy Secretary of Defense with a recommendation for approval or disapproval.

(b) This coordination will carefully consider if the capability or information being apportioned still requires SAP protections or if, in part or in whole, the capability or information could be adequately protected outside of SAP channels.

(c) Additionally, if not already approved for disclosure to foreign governments, this coordination will also consider if the SAP capability or information should be disclosed to foreign governments in accordance with Section 8.

(4) CA SAPCO directors will nominate SAP-protected capabilities or information for apportionment through the IJSTO process no later than 18 months before planned initial operational capability or as soon as the capability has been tested and deemed operationally effective, whichever occurs first. Additionally, if a non-apportioned DoD SAP-protected capability is operationally available to the CCMDs, the CA SAPCO will nominate it for apportionment, or submit a waiver request, at the earliest opportunity.

(5) The CA may submit a request to waive the apportionment requirement to the Director, DoD SAPCO. The Director, DoD SAPCO will coordinate the request through the SSWG and submit it to the appropriate OA and the Vice CJCS for approval or disapproval. When requesting an apportionment waiver, the CA will recommend a process by which the CCMDs will integrate the SAP-protected capability during joint planning and operations, including recommended deployment and employment approval authorities for capabilities.

c. SAP-Protected Capability Deapportionment.

(1) When apportioned SAP-protected capabilities or information will no longer be available to CCDRs for joint planning and operations, CAs will submit a deapportionment request to the JS in accordance with procedures established by the CJCS.

(2) The JS will submit the deapportionment request to the Director, DoD SAPCO. The Director, DoD SAPCO will coordinate it through the SSWG, the SRG, and the SAPOC, as required, and submit it to the Deputy Secretary of Defense with a recommendation for approval or disapproval.

(3) If applicable, the CAs will complete deapportionment of SAP-protected capabilities or information before initiating any disestablishment activities.

d. Modification of Authorities for Apportioned SAP-Protected Capabilities and Information.

(1) When changes to the authorities for the deployment or employment of an apportioned SAP-protected capability or information are required or desired, the JS will submit an apportionment modification request to the Director, DoD SAPCO in accordance with procedures established by the CJCS.

(2) When submitting a request for modification of authorities, the JS will provide the rationale for the modification.

(3) The Director, DoD SAPCO will coordinate the request through the SSWG, the SRG, and the SAPOC, as required, and submit it to the Deputy Secretary of Defense with a recommendation for approval or disapproval.

(4) For capabilities or information that no longer require SAP protection, the modification of approval authorities must be completed before initiating any disestablishment activities.

(5) When SAP-protected capabilities or information are no longer relevant to CCMD planners or no longer require SAP protection, CAs will follow the procedures in Paragraph 4.2. to remove it from the SAP protecting it.

SECTION 7: CONGRESSIONAL SAP PROCEDURES

7.1. GENERAL PROCEDURES.

a. All DoD employees accessed to DoD SAPs will coordinate with and notify the DoD and OA SAPCOs through the CA SAPCO when intending to brief or provide DoD SAP material to any appropriately accessed members of Congress or professional staff member in accordance with DoDD 5205.07.

b. The Director, DoD SAPCO will manage the proper delivery and receipt of all DoD SAP materials to appropriately accessed personnel on the defense and intelligence committees in coordination with the Assistant Secretary of Defense for Legislative Affairs and the Deputy Comptroller for Budget and Appropriations Affairs in the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense as necessary, in accordance with DoDI 5545.02.

7.2. CONGRESSIONAL SAP ACCESS.

a. General Access Provisions.

(1) Only members of Congress and professional staff who meet the SAP access prerequisites described in Paragraph 5.1. and the further provisions described in this section may be given access to SAP-protected material or receive SAP briefings.

(2) DoD SAPCO will complete the PAR and manage access for all members of Congress and professional staff members requiring access to a SAP. When a member of Congress or a professional staff member is given access to a SAP umbrella, that member of Congress or professional staff member will also be given access to all compartments and sub-compartments that fall under the respective SAP umbrella, with the exception of waived sub-compartments as described in Paragraph 7.2.a.(3).

(3) Only the chair, the ranking member, the staff directors, and one designated security manager of the defense and intelligence committees will be authorized access to waived DoD SAPs within their committee's respective oversight jurisdiction. Requests to access additional members of Congress or professional staff must be approved by the Secretary of Defense or Deputy Secretary of Defense.

b. Committee Members.

Members of Congress assigned to the defense and intelligence committees are authorized access to all DoD SAPs within the respective committee's SAP oversight jurisdiction, except for waived programs as described previously. The intelligence committees are authorized access only to those DoD SAPs designated by the Secretary of Defense or Deputy Secretary of Defense as intelligence or intelligence related.

c. Professional Staff Members.

(1) One professional staff member for both the majority and the minority party of the defense and intelligence committees may be granted access to all non-waived SAPs within the respective committee's SAP oversight jurisdiction. The staff director and the minority staff director of the committees request individual professional staff member SAP access to non-waived SAPs on behalf of the chair and ranking member. Access will be approved by the Director, DoD SAPCO to ensure compliance with personnel security requirements.

(2) No later than March 1 of each year, DoD SAPCO will obtain updated information on the access status of professional staff members from the staff directors of the defense and intelligence committees. DoD SAPCO will coordinate with the staff directors on employment changes so that the DoD can initiate the appropriate de-access procedures.

d. Non-Committee Members of Congress and Professional Staff Members.

Members of Congress and professional staff members not assigned to the defense or intelligence committees may be granted access to non-waived DoD SAPs by the Director, DoD SAPCO following consultation with the respective chamber of Congress chair and ranking defense committee members. If either the chair or ranking member objects to such access, the Secretary of Defense or Deputy Secretary of Defense will decide if access will be granted.

e. Senate and House Leadership Professional Staff.

The Senate Majority Leader, the Senate Minority Leader, the Speaker of the House, and the Minority Leader of the House may each nominate one professional staff member who is eligible for SAP access to be accessed to all DoD SAPs. Access will be approved by the Director, DoD SAPCO to ensure compliance with personnel security requirements.

f. Personal Staff.

The personal staff of a member of Congress will not be granted access to DoD SAPs.

g. Government Accountability Office (GAO).

Authorized DoD AAAs may grant SAP access to SAP eligible staff of the GAO for specific projects. Before granting SAP access to GAO staff, the Director, DoD SAPCO will consult with the chairman and ranking defense committee members, unless the GAO is already tasked with a SAP-related action in existing legislation.

h. Congressional Budget Justification Materials.

The DoD will conform to all congressional reporting requirements. The DoD will submit to the congressional defense and intelligence committees such additional materials as are requested by the committees and are within the jurisdiction of each committee. Justification materials for waived programs will be presented only to the committee staff directors.

i. Physical Security Procedures.

The Director, DoD SAPCO accredits SAPFs in the U.S. Capitol complex and will work closely with the congressional defense and intelligence committees to ensure adequacy of the physical custody procedures in practice by the committees for handling and storage of SAP materials and information.

SECTION 8: SAP ENTERPRISE INTERNATIONAL COOPERATION

8.1. GENERAL.

DoD SAP information will be shared with foreign governments to the greatest extent practical, consistent with National Defense Strategy guidance.

8.2. SAP ACCESS REQUIREMENTS FOR FOREIGN NATIONALS.

a. Before the release of SAP information to a foreign government, a general security of military information agreement (GSOMIA) or general security of information agreement (GSOIA) must be in place with that foreign government. These legally binding agreements establish terms for the protection and handling of classified military information (GSOMIA) or other government information (GSOIA) provided by either partner to the other. If there is no GSOIA or GSOMIA, provisions may be included in an MOU, MOA (e.g., for cooperative agreements), or a program specific security agreement (e.g., for foreign military sales cases).

(1) Additionally, a separate DoD agreement is required to ensure foreign governments receiving the information maintain equivalent SAP security standards, policies, and processes as the DoD.

(2) These agreements will detail the security procedures governing access to and exchange of SAP information.

(3) DoD Components will negotiate the agreements in coordination with the Director, DoD SAPCO and in accordance with DoDI 5530.03.

b. To receive DoD SAP information, individual foreign nationals must maintain an equivalent level of clearance and access to classified information based upon the commensurate U.S. standards identified in Paragraph 5.1., and SAP access agreements negotiated with the foreign government.

8.3. SAP FOREIGN DISCLOSURE PROCEDURES.

a. Only the Secretary of Defense and Deputy Secretary of Defense may approve the disclosure of SAP information to foreign governments, unless otherwise delegated. All disclosure of DoD SAP information to foreign governments will be in accordance with National Disclosure Policy-1.

b. SAP OAs and CAs will submit SAP foreign disclosure requests to the Secretary of Defense or Deputy Secretary of Defense through the Director, DoD SAPCO. Foreign disclosure request packages will include, at minimum:

(1) PSA or DoD Component head endorsement. PSAs or DoD Component heads may delegate this endorsement authority to their principal deputies.

(2) Draft action memo for Secretary of Defense or Deputy Secretary of Defense approval. The draft action memo will address the SAP information requested for release, the foreign government(s) to receive access to the information, the number of foreign government billets authorized to receive the information, delegation of AAA, delegation of billet management with a maximum number of billets authorized, and other information deemed necessary for the Secretary of Defense or Deputy Secretary of Defense to make a decision.

(3) Draft core documents. Core documents for the request package include the program or activity quad chart, indoctrination briefing, and recommended SCG annex updates. This is to ensure that the foreign governments receiving DoD SAP information know how to protect the information furnished to them.

(4) Other information. The package will include relevant decision memorandums from other DoD authorities, as well as other documentation deemed necessary for the Secretary of Defense and Deputy Secretary of Defense to make a decision.

c. Following Secretary of Defense or Deputy Secretary of Defense approval to disclose SAP information to a foreign government(s), the DoD Component may disclose the information to foreign governments in accordance with DoDD 5230.11 and component foreign disclosure procedures.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
AAA	access approval authority
CA	cognizant authority
CCDR	Combatant Commander
CCMD	Combatant Command
CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
CPI	critical program information
CUI	controlled unclassified information
DCSA	Defense Counterintelligence and Security Agency
DNI	Director of National Intelligence
DoDD	DoD directive
DoDI	DoD instruction
DoDM	DoD manual
E.O.	Executive order
GAO	Government Accountability Office
GSOIA	general security of information agreement
GSOMIA	general security of military information agreement
IC	Intelligence Community
IJSTO	integrated joint special technical operations
JF	joint force
JS	Joint Staff
JTF	joint task force
MOA	memorandum of agreement
MOU	memorandum of understanding
NTK	need to know
OA	oversight authority
OPR	office of primary responsibility
PAR	program access request
PSA	Principal Staff Assistant

ACRONYM	MEANING
SAP	special access program
SAPCO	Special Access Program Central Office
SAPCON	special access program control
SAPF	special access program facility
SAPOC	Special Access Program Oversight Committee
SCG	security classification guide
SRG	Senior Review Group
SSWG	Special Access Program Senior Working Group
TR	Transitional Repository
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering
USD(P)	Under Secretary of Defense for Policy

G.2. DEFINITIONS.

TERM	DEFINITION
acknowledged SAP	A SAP whose existence is acknowledged, affirmed, or made known to others, but its specific details (e.g., technologies, materials, techniques) are classified as specified in the applicable SCG.
apportionment	Provision of a capability or information to operational forces through the IJSTO process. Apportionment grants CCDRs the authority to plan for deployment and employment of SAP-protected capabilities and information and establishes the approval authority for deployment and employment.
archive	Continued provision of SAP protections for CPI no longer actively used by the DoD but deemed to be of such a sensitive nature that continued SAP protections are warranted.
CA	The DoD Component head described in DoDD 5100.01 or a PSA with significant equity in SAP governance and execution, who the Secretary of Defense or Deputy Secretary of Defense has designated in writing as a CA.
carve out	A provision approved by the Secretary of Defense or Deputy Secretary of Defense that relieves DCSA of its National Industrial Security Program obligation to perform industrial security oversight functions for a DoD SAP.

TERM	DEFINITION
content SAP	A SAP that protects discrete CPI.
CPI	Defined in DoDI 5200.39. For the purposes of this issuance, all references to CPI are for CPI requiring SAP protection.
deapportionment	Through the IJSTO process, a decision by the Secretary of Defense or Deputy Secretary of Defense that removes the authority of CCDRs to plan for the deployment and employment of SAP-protected capabilities and information.
disestablishment	Cancellation of active use and management of a SAP. Disestablishment may result in archiving if the CPI warrants continued SAP protections.
establishment	Initiation of SAP protections. Establishment may result in the addition of a new SAP umbrella, compartment, or sub-compartment to the SAP architecture or addition of CPI associated with sensitive capabilities or information to the protections of an existing SAP.
horizontal protection	Consistent application of safeguards for similar or associated CPI within DoD SAPs.
IJSTO process	The process by which the CCMDs integrate DoD, other U.S. agency, and international capabilities and information protected by DoD SAPs into joint planning, exercises, and operations and obtain Presidential or Secretary of Defense authorization for operational use of the capabilities and information.
inclusion	The process of sharing CPI on SAP capabilities or information with CCMDs for awareness and understanding. Inclusion provides information about capabilities but does not provide any authority to deploy or employ the capabilities.
JF	Joint DoD Components, including JS, CCMDs, sub-unified commands, joint functional component commands, JTFs, and the National Guard Bureau.
JF integration SAP	A SAP intended for greater integration and sharing across the JF and the broader SAP community.
OA	The designated official assigned oversight responsibility for a SAP.

TERM	DEFINITION
SAP	A system of enhanced security measures for sensitive capabilities or information that imposes safeguarding and access requirements exceeding those normally required for information at the same classification level.
SAP compartment	A tier 2 element of the SAP architecture, subordinate to a SAP umbrella.
SAP Enterprise	The collective personnel, organizations, programs, processes, and systems that use and manage DoD SAP-protected information.
SAPF	A facility accredited for processing, handling, discussing, or storing SAP-protected CPI.
SAP sub-compartment	An element of the SAP architecture at tier 3 and below, subordinate to a SAP compartment.
SAP type	Designation of a SAP as either acknowledged or unacknowledged.
SAP umbrella	A tier 1 ~~s~~tructural grouping within the SAP architecture.
stakeholder	A CA whose DoD Component uses a SAP to protect CPI associated with its sensitive capabilities or information. The CA is a stakeholder in the particular SAP being used for protections.
strategic enabler SAP	A SAP protecting capabilities or information that enable strategic competition and warrant more limited and restrictive sharing than JF integration SAPs.
structural SAP	A SAP that provides organization to the architecture and does not protect discrete CPI.
TR umbrella	An enduring DoD SAP umbrella that temporarily groups DoD SAPs during establishment or disestablishment.
unacknowledged SAP	A SAP having enhanced security measures, ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.
waived SAP	A SAP for which the Secretary of Defense has waived applicable reporting following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls than other unacknowledged SAPs.

REFERENCES

Code of Federal Regulations, Title 32, Part 117 (also known as the "National Industrial Security Program Operating Manual")

Code of Federal Regulations, Title 36

Department of Defense, "National Defense Strategy," current edition

DoD Directive 3020.40, "Mission Assurance (MA)," November 29, 2016, as amended

DoD Directive 5100.01, "Functions of the Department of Defense and Its Major Components," December 21, 2010, as amended

DoD Directive 5105.79, "DoD Senior Governance Framework," November 8, 2021

DoD Directive 5144.02, "DoD Chief Information Officer," November 21, 2014, as amended

DoD Directive 5205.07, "Special Access Program Policy," September 12, 2024

DoD Directive S-5210.36, "(U) Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government," November 6, 2008, as amended

DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," November 7, 2023

DoD Directive 5240.02, "Counterintelligence (CI)," March 17, 2015, as amended

DoD Instruction 4000.19, "Support Agreements," December 16, 2020

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, 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 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 5530.03, "International Agreements," December 4, 2019

DoD Instruction 5545.02, "DoD Policy for Congressional Authorization and Appropriations Reporting Requirements," December 19, 2008

DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, as amended

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

DoD Manual 8180.01, "Information Technology Planning for Electronic Records Management," August 4, 2023

Executive Order 11858, "Foreign Investment in the United States," May 7, 1975

Executive Order 13526, "Classified National Security Information," December 29, 2009

Intelligence Community Directive 906, "Controlled Access Programs," October 17, 2015

National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 2, 2002

National Security Directive 42, "National Policy for the Security of National Telecommunications and Information Systems," July 5, 1990

United States Code, Title 10

United States Code, Title 44