DoD Directive 5205.07

Special Access Program Policy

Originating Component:	Office of the Performance Improvement Officer / 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 Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended
Incorporates and Cancels:	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 provides governance structure for the oversight and management of all DoD special access programs (SAPs) in accordance with Executive Order (E.O.) 13526.
- Establishes the Special Access Program Oversight Committee (SAPOC), Senior Review Group (SRG), Special Access Program Senior Working Group (SSWG), and DoD Special Access Program Central Office (SAPCO).

TABLE OF CONTENTS

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, the Combatant Commands (CCMDs), 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 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 departments, activities, agencies, and all other organizational entities that require access to DoD SAPs pursuant to the terms and conditions of a memorandum of agreement or other interagency agreement established with the DoD.

1.2. POLICY.

a. The DoD will establish and apply SAP security protection to classified national security information in accordance with E.O. 13526; Part 2001 of Title 32, Code of Federal Regulations; DoD Instruction (DoDI) 5200.01; and DoD Manual 5200.01 to safeguard the DoD's most sensitive classified information related to advanced systems, capabilities, technologies, and operations from adversary knowledge when:

(1) The vulnerability of, or threat to, specific information is exceptional and collateral security requirements are deemed insufficient; or

(2) Required by statute.

b. SAP-protected capabilities and information are key enablers to gain and maintain enduring military advantages for the current and future Joint Force. DoD Components will integrate these capabilities and sets of information across the Joint Force and will maximize prompt apportionment of SAP capabilities and information to ensure effective U.S. warfighting advantages during times of conflict.

c. The DoD will have SAP oversight authorities (OAs) to oversee SAPs for which the OA has responsibility. All DoD SAPs will be assigned to an OA for oversight purposes. DoD SAP OAs are 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)), Under Secretary of Defense for Intelligence and Security (USD(I&S)), and the Director, DoD SAPCO.

d. The DoD will have SAP cognizant authorities (CAs) to manage the use of SAP protection for critical program information (CPI) related to capabilities and information for which the CA has responsibility. CAs are the Principal Staff Assistants and DoD Component heads described in DoD Directive (DoDD) 5100.01 with significant equity in the management and execution of SAP protections, whom the Secretary of Defense or Deputy Secretary of Defense has designated in writing as CAs.

e. The Director, DoD SAPCO, under the authority, direction, and control of the Deputy Secretary of Defense, will be a general officer, flag officer, or Senior Executive Service member or equivalent appointed to oversee day-to-day management of the SAP Enterprise. The Director, DoD SAPCO reports directly to the Deputy Secretary of Defense.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, DOD SAPCO.

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

a. Serves as the:

(1) DoD-designated proponent for developing and implementing policies and procedures for DoD SAP execution, management, administration, oversight, and governance.

(2) Executive Secretary of the SAPOC and SRG and as Chair of the SSWG.

(3) OA for SAPs as designated by the Deputy Secretary of Defense, including those protecting capabilities and information shared with the DoD by foreign governments.

(4) CA for:

(a) SAPs as designated by the Deputy Secretary of Defense.

(b) DoD Components not supported by another SAPCO.

(c) Capabilities and information shared with the DoD by foreign governments.

(d) SAP studies, portfolios, and associated access management structures involving DoD SAPs.

(5) DoD primary point of contact for SAP matters with agencies of the Executive Branch, the Judicial Branch, and the Legislative Branch, including support to SAP congressional meetings, hearings, and responses to congressional inquiries, unless otherwise specified by statute or regulation.

(6) Executive Secretary of the Special Technical Activities Oversight Committee pursuant to the November 21, 2020 Deputy Secretary of Defense Memorandum.

b. Publishes and maintains security classification guides for all DoD SAP umbrellas in accordance with DoD Manual 5200.45. The Director, DoD SAPCO has jurisdiction over the protection of information contained within DoD SAPs and is delegated TOP SECRET original classification authority for all DoD SAP information for purposes of issuing SAP security classification guides.

c. Coordinates and provides guidance for annual SAP reviews and reports in accordance with E.O. 13526 and congressional review and reporting requirements.

d. Maintains a single, authoritative repository for DoD SAP personnel access and SAP facility (SAPF) accreditation.

e. Accredits congressional SAPFs. Maintains records of DoD SAP information provided to Congress.

f. Coordinates SAP actions with the OAs before:

(1) Forwarding the actions to the Deputy Secretary of Defense.

(2) Coordinating, discussing, or exposing SAP information outside the DoD.

g. Implements procedures for sharing DoD SAP-protected information with foreign governments in accordance with DoDD 5230.11 and DoDI 5530.03, including facilitating and maintaining international agreements for foreign government involvement with DoD SAPs.

h. Develops and manages a SAP process for governing specialized activities (e.g., Defense Contract Audit Agency audits, technical security countermeasures, polygraph examinations, and joint inspection activities) in support of all DoD SAPs and protects those processes using appropriate safeguards in coordination with the USD(I&S). This process allows personnel to access the level of information necessary to perform their duties while limiting the need for detailed briefings.

i. Coordinates with the USD(I&S) to ensure DoD issuances appropriately reflect SAP security requirements.

j. Coordinates with all OAs and informs CA SAPCO directors before acting on any significant security issues that may adversely impact SAPs unless constrained by higher authority.

k. Notifies:

(1) The Deputy Secretary of Defense and the USD(I&S) of significant security incidents involving SAP information in accordance with DoD Manual 5200.01.

(2) All SAPCO directors of suspensions, revocations, and reinstatements of SAP access.

l. Reports to the SAPOC annually on approved SAPFs. The report is categorized by installation, contractor location, and international affiliation.

m. Coordinates with the Executive Secretaries of the Secretary of Defense and Deputy Secretary of Defense governance forums to ensure SAP issues prepared for those forums are staffed and presented with the appropriate security control measures and procedures in accordance with DoDD 5105.79.

n. Provides administrative and management support to OSD-level executive committees for SAP matters.

2.2. USD(R&E).

The USD(R&E):

a. Serves as the OA for SAPs as designated by the Deputy Secretary of Defense and fulfills OA responsibilities in accordance with DoDI 5205.11.

b. As the DoD Chief Technology Officer, develops and coordinates DoD SAP guidance related to advancing technology and innovation within the DoD and internationally in coordination with the Director, DoD SAPCO and in accordance with DoDD 5137.02.

c. Manages and oversees all DoD SAP science and technology and ensures alignment to science and technology strategy and technology overmatch goals through periodic reviews and technology modernization transition reviews pursuant to DoDD 7045.20.

2.3. USD(A&S).

The USD(A&S):

a. Serves as the OA for SAPs as designated by the Deputy Secretary of Defense and fulfills OA responsibilities in accordance with DoDI 5205.11.

b. Manages, administers, executes, and establishes policy for the SAP Corporate Portfolio Program.

c. Conducts and chairs integrated acquisition portfolio reviews for SAP-protected capabilities in accordance with DoDD 7045.20.

2.4. USD(P).

The USD(P):

a. Serves as the OA for SAPs as designated by the Deputy Secretary of Defense and fulfills OA responsibilities in accordance with DoDI 5205.11.

b. Ensures SAPs are integrated into and consistent with the development of national security and defense strategies, plan development, and contingency operations through oversight of the Integrated Joint Special Technical Operations (IJSTO) process.

c. Ensures capabilities and information protected by DoD SAPs are approved for inclusion and apportioned at the earliest opportunity in collaboration with the Vice Chairman of the Joint Chiefs of Staff in accordance with DoDI 5205.11. To accomplish this, the USD(P):

(1) Ensures the SAP architecture has the appropriate operational compartments and sub-compartments for SAP capabilities in coordination with the Director, DoD SAPCO, in accordance with the procedures in DoDI 5205.11.

(2) Ensures SAP capabilities and information are approved for inclusion in the appropriate SAPs when they become relevant to CCMD planners, in accordance with DoDI 5205.11.

(3) Reviews the mission ready status of SAP capabilities apportioned through the IJSTO process.

(4) Develops guidance for the deployment and execution authorities of apportioned SAP capabilities for the purpose of prioritizing low-density and high-demand capabilities, highly sensitive capabilities, and capabilities that should be reserved for specific contingencies. Evaluates the proposed deployment and execution authorities of capabilities during the apportionment process to ensure DoD Components are making recommendations for authorities in accordance with this issuance.

(5) Oversees apportionment decision-making processes for capabilities and information that have both SAP and collateral lines of effort.

(6) Facilitates the transfer of apportionment of SAP capabilities and information out of the IJSTO process to non-SAP decision-making processes, when required.

d. Executes responsibilities assigned for SAP matters involving the National Security Council in coordination with the Director, DoD SAPCO in accordance with DoDD 5111.01.

e. Operates the OSD Special Technical Operations cell to coordinate and process OSD participation in IJSTO. This includes approving the appropriate SAP access for non-DoD departments and agencies for the development and approval of plans in IJSTO unless the Deputy Secretary of Defense specifically assigns approval to another SAP OA or CA.

f. Develops, coordinates, provides, and oversees the implementation of special security countermeasures policy, including countermeasures associated with arms control and non-proliferation initiatives that could impact DoD SAPs.

2.5. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO).

The USD(C)/CFO, using the SAP governance structure:

a. Leads all budget and execution reviews for DoD-funded capabilities and information activities protected by DoD SAPs.

b. Develops and provides budget call and guidance preparation instructions for all SAP budget submissions, including reprogramming actions and mid-year and other program execution reviews.

2.6. USD(I&S).

The USD(I&S):

a. Serves as the OA for SAPs as designated by the Deputy Secretary of Defense and fulfills OA responsibilities in accordance with DoDI 5205.11.

b. As the DoD Senior Security Official, in coordination with the Director, DoD SAPCO, develops, coordinates, and establishes DoD SAP security policy and provides security oversight:

(1) Of the DoD Components that manage SAP equities.

(2) With industry as it relates to industrial security oversight responsibilities delegated by the Secretary of Defense.

c. Monitors the investigation of counterintelligence matters, security violations, or infractions involving DoD SAPs in coordination with the Director, DoD SAPCO.

d. Serves as the primary interface for the Office of the Director of National Intelligence (ODNI) and members of the Intelligence Community (IC), including sharing with the DoD compartmented capabilities and information intended for inclusion and subsequent apportionment. In this role, serves as the OA for the DoD SAP that protects the shared compartmented capability or information. The CA for the DoD SAP will be:

(1) The DoD Component head, if the compartmented capability or information is shared by a DoD Component that is an element of the IC.

(2) The USD(I&S), if the compartmented capability or information is shared by a DoD Component that is **not** an element of the IC.

e. Prescribes guidance on the handling, discussion, display, and processing of DoD SAP information in any accredited sensitive compartmented information facility. This guidance is revised as necessary to promote effective cooperation between the DoD and other U.S. Government organizations authorized to establish SAPs, as described in E.O. 13526.

f. Carries out the responsibilities assigned in DoDD 5143.01 for SAP matters involving the ODNI and IC members in coordination with the Director, DoD SAPCO.

g. Oversees an education and training program for SAP professionals in collaboration with the Director, DoD SAPCO and the Director, Defense Counterintelligence and Security Agency (DCSA), through the Center for the Development of Security Excellence.

h. Executes the responsibilities for SAP matters involving National Security Council intelligence programs, in accordance with DoDD 5143.01.

i. Serves as the primary interface to the Information Security Oversight Office regarding policies and regulations affecting DoD SAPs and maintaining the file series exemptions for DoD SAPs in accordance with E.O. 13526.

2.7. DIRECTOR, DCSA.

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

a. Develops SAP-related training courses and maintains a cadre of personnel proficient in SAP policies, procedures, and security to support all aspects of SAP training and education.

b. Supports the professional development and certification of SAP security professionals in coordination with the DoD SAPCO and OA and CA SAPCOs.

2.8. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE (GC DOD).

The GC DoD:

a. Provides legal advice, as it relates to DoD SAPs, to the SAP governance and oversight structure and to other DoD entities as required.

b. Provides legal reviews of SAP project plans that result in establishment of a new SAP umbrella, compartment, or sub-compartment in accordance with DoDI 5205.11.

2.9. DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION (DCAPE).

The DCAPE:

a. Serves as the principal advisor to the Secretary of Defense and other senior DoD officials to provide independent analysis and advice on the cost of capabilities protected by SAPs within the DoD. Evaluates and conducts studies considering current and projected threats, estimated costs, resource constraints, and U.S. defense objectives and priorities.

b. Helps develop direction and guidance for DoD SAPs to address programmatic funding requirements and resolve issues that arise.

c. Develops and provides preparation instructions for DoD SAP program objective memorandum submissions.

d. Coordinates SAP issues prepared for the DoD senior governance forums with the Director, DoD SAPCO in accordance with DoDD 5105.79.

2.10. DIRECTOR OF OPERATIONAL TEST AND EVALUATION.

The Director of Operational Test and Evaluation identifies acquisition SAPs for operational test and evaluation oversight in coordination with USD(A&S) and USD(R&E) SAPCOs.

2.11. DOD CHIEF INFORMATION OFFICER (DOD CIO).

The DoD CIO:

a. Resources, develops, installs, and maintains information technology (IT) systems and secure network capabilities and services for processing SAP information in response to CA requirements. Enables sharing of SAP-protected data and metadata and collaboration among users of DoD SAPs, including DoD Components, the IC, other SAP-owning U.S. Government organizations, industry partners, and foreign governments. Collects and securely destroys SAP IT equipment when it is removed from service.

b. Establishes and administers governance and risk management policies to develop SAP IT, data, and metadata strategy and policy; telecommunications infrastructure policy; SAP network IT and data requirements; and network and systems funding oversight policy in coordination with the Director, DoD SAPCO.

c. Develops and issues supplemental guidance for assessment and authorization of DoD SAP information systems; data and metadata sharing; and strengthening cybersecurity in coordination with the Director, DoD SAPCO and in accordance with requirements established by the National Manager for National Security Systems pursuant to National Security Directive 42 and DoDD 5144.02.

d. Develops policies and procedures related to the management of SAP records for the DoD, including long-term retention and storage of SAP records in coordination with the OSD Records Administrator and the Director, DoD SAPCO pursuant to Chapters 31 and 33 of Title 44, United States Code, and in accordance with Parts 1220-1228 of Title 36, Code of Federal Regulations and DoDI 5015.02.

e. Partners with the ODNI to jointly manage DoD SAP and interagency SAP IT systems integration, including processing of IC SAP information on DoD SAP-authorized IT systems, in coordination with the Director, DoD SAPCO.

2.12. ASSISTANT TO THE SECRETARY OF DEFENSE FOR PRIVACY, CIVIL LIBERTIES, AND TRANSPARENCY.

The Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency ensures audit functions are performed pursuant to DoDD 5148.13.

2.13. CJCS.

The CJCS:

a. Develops, maintains, and executes the IJSTO process. The IJSTO process includes a coordination procedure for gaining President of the United States or Secretary of Defense approval, when required, to deploy and employ capabilities protected by DoD SAPs. Those procedures include consultation with the Military Departments, appropriate CCMDs, and the IC

for assessments. The CJCS uses the IJSTO process to apportion SAP-protected capabilities and information, not the SAPs that protect them.

b. Establishes an office to review and disseminate planning information concerning the operational aspects of apportioned SAPs.

c. Maintains a capability to rapidly establish and accredit SAPFs in support of contingency operations.

d. Ensures the availability of an authorized information system to facilitate the IJSTO process and coordination and information sharing with foreign governments in coordination with the DoD CIO.

e. Provides guidance to capability providers for efficient inclusion, apportionment, and deapportionment of DoD SAP-protected capabilities and information to enable effective integration into CCMD plans and operations.

f. Schedules and chairs capability portfolio management reviews for SAP-protected capabilities in accordance with DoDD 7045.20.

SECTION 3: SAP GOVERNANCE

3.1. GENERAL.

a. DoD SAP governance will use an enterprise framework with a uniform and enduring structure that anticipates future requirements, enables greater innovation, facilitates collaboration with appropriately accessed partners, and enables the rapid application of SAP protection as new capabilities or information arise.

b. The SAP architecture will be organized into SAP umbrellas that group similar CPI to facilitate sharing and collaboration. Each umbrella will be further organized into SAP compartments and sub-compartments. DoD Components will work with the Director, DoD SAPCO, and OAs, via the SAP governance bodies, to integrate new information proposed for SAP protection into the enduring SAP architecture to the greatest extent practical. The DoD SAP architecture will use an enduring structure to facilitate efficient use and oversight.

c. The SAP architecture and related management procedures will distinguish between Joint Force Integration SAPs and Strategic Enabler SAPs.

d. Establishment of new SAP umbrellas and compartments will be by exception. Establishment of SAPs to protect new and novel CPI at all tiers of the SAP architecture requires Secretary of Defense or Deputy Secretary of Defense approval.

e. Initial access to DoD SAPs will be strictly controlled, based on broad collaboration and shared risk within the SAP Enterprise. Access to a SAP will be strictly limited to the minimum number of personnel necessary. Granting initial access to a SAP will be based solely upon a determination that the individual:

(1) Has a valid need to know (NTK).

(2) Has the necessary security clearance.

(3) Meets approved personnel security prerequisites.

(4) Will contribute to program execution or oversight.

f. Determination of NTK will consider an individual's role and potential participation in separate but related SAPs. To enable collaboration and facilitate greater innovation, personnel with NTK may be accessed to similar information throughout the SAP architecture (e.g., science and technology or operations).

g. All personnel accessed to DoD SAPs will notify the Director, DoD SAPCO and OA SAPCO directors through their SAP CA SAPCO in a timely fashion when briefing or providing DoD SAP material to any member of Congress or their staff. No DoD contractor entity, contractor employee, contractor representative, or consultant will provide SAP material to any members of Congress or their staff without Director, DoD SAPCO approval.

h. Multiple CAs may use the same DoD SAP to protect similar CPI associated with the CAs' sensitive capabilities or information. A CA whose component uses a SAP to protect its sensitive capabilities or information is a stakeholder in that SAP.

3.2. DOD SAP GOVERNANCE BODIES.

Effective governance relies on disciplined processes, consistency, transparency, accuracy, and timeliness. The SAP governance structure consists of the SAPOC, the SRG, and the SSWG. These bodies will advise and assist the Secretary of Defense and Deputy Secretary of Defense in the governance, management, administration, and oversight of DoD SAPs in accordance with DoDI 5205.11.

a. SAPOC.

(1) The SAPOC is the senior governing body of the DoD SAP Enterprise for governance, management, and oversight of DoD SAPs. It will ensure SAPs meet warfighter needs while protecting CPI.

(2) SAPOC members are the:

(a) Deputy Secretary of Defense, serving as the Chair.

(b) Director, DoD SAPCO, serving as the Executive Secretary.

(c) USD(R&E).

(d) USD(A&S).

(e) USD(P).

(f) USD(C)/CFO.

(g) USD(I&S).

(h) Vice Chairman of the Joint Chiefs of Staff.

(i) GC DoD.

(j) DCAPE.

(k) DoD CIO.

(l) Under Secretaries of the Army, Navy, and Air Force.

(m) Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.

(n) Vice Chiefs of Staff of the Army and the Air Force.

(o) Assistant Commandant of the Marine Corps.

(p) Vice Chiefs of Naval Operations and Space Operations.

b. SRG.

(1) The SRG serves as a supporting tier forum for the SAPOC. Its primary function is to resolve disagreements among DoD Components participating in the SSWG and review information destined for the SAPOC. The SRG has no designated individual as the Chair. SRG participants have inherent authorities that affect SRG governance, and these are exercised in each member's individual capacity.

(2) SRG members are:

(a) Director, DoD SAPCO serving as the Executive Secretary.

(b) Representatives that each SAPOC member designates in writing.

(c) Additional appropriately cleared personnel, if the Director, DoD SAPCO approves.

c. SSWG.

(1) The SSWG is the working-level governance, collaboration, and action body of the DoD SAP Enterprise.

(2) Voting SSWG members are:

(a) The Director, DoD SAPCO, serving as the Chair.

(b) The SAPCO directors (one representing each organization) for the Offices of the USD(R&E), USD(A&S), USD(P), and USD(I&S); the Military Departments; the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict; and the Joint Staff.

(3) Non-voting members include the principal-appointed representatives from the Offices of the USD(C)/CFO, GC DoD, DCAPE, and DoD CIO, and the United States Marine Corps.

(4) Other participants may be invited at the Chair's discretion for relevant discussions.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CA	cognizant authority
CCMD	Combatant Command
CJCS	Chairman of the Joint Chiefs of Staff
CPI	critical program information
DCAPE	Director, Cost Assessment and Program Evaluation
DCSA	Defense Counterintelligence and Security Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
E.O.	Executive order
GC DoD	General Counsel of the Department of Defense
IC	Intelligence Community
IJSTO	Integrated Joint Special Technical Operations
IT	information technology
NTK	need to know
OA	oversight authority
ODNI	Office of the Director of National Intelligence
SAP	special access program
SAPCO	Special Access Program Central Office
SAPF	special access program facility
SAPOC	Special Access Program Oversight Committee
SRG	Senior Review Group
SSWG	Special Access Program Senior Working Group
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
apportionment	Formally providing a SAP-protected capability or information to CCMDs via the IJSTO process for use during deliberate planning, crisis action response, and operational employment.
CA	The head of a DoD Component described in DoDD 5100.01 or a Principal Staff Assistant with significant equity in the management and execution of SAP protections, whom the Secretary of Defense or Deputy Secretary of Defense has designated in writing as a CA.
CPI	Defined in DoDI 5200.39. For the purposes of this issuance, all references to CPI are for CPI requiring SAP protection.
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.
inclusion	The process of sharing CPI associated with SAP-protected capabilities or information with CCMDs and Military Services for awareness and understanding. Inclusion provides information about the capability but does not provide any authority to plan, deploy, or employ the capability.
Joint Force	Joint DoD Components, including the Joint Staff, CCMDs, sub-unified commands, joint functional component commands, joint task forces, and the National Guard Bureau.
Joint Force Integration SAP	A SAP intended for greater integration and sharing across the Joint Force and the broader SAP community.
memorandum of agreement	Written agreement among relevant parties that specifies roles, responsibilities, terms, and conditions for each party to reach a common goal. A memorandum of agreement is required when SAP resources are committed between DoD and non-DoD components.
OA	The designated official assigned oversight responsibility for a SAP.
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 level.

TERM	DEFINITION
SAP architecture	The tiered structure for organizing DoD SAPs, composed of SAP umbrellas, compartments, and sub-compartments.
SAP compartment	A tier 2 element of the SAP architecture subordinate to a SAP umbrella.
SAP Corporate Portfolio Program	A DoD program that enables U.S. defense corporations to address current and future national security challenges in a responsive, collaborative, and cost-efficient manner.
SAP Enterprise	The collective personnel, organizations, programs, processes, and systems that use and protect DoD SAP information.
SAP project plan	A plan for placement of newly identified CPI into the SAP architecture, created by the initiating CA and submitted to the SSWG for review and approval.
SAP sub-compartment	An element of the SAP architecture at tier 3 and below, subordinate to a SAP compartment.
SAP umbrella	A tier 1 structural grouping of related CPI within the SAP architecture.
stakeholder	A CA whose component uses a SAP to protect CPI associated with its sensitive capabilities or information. The CA is a stakeholder in the 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 Joint Force Integration SAPs.
tier	A sequential level of organization within the SAP architecture.

REFERENCES

Code of Federal Regulations, Title 32, Part 2001
Code of Federal Regulations, Title 36
Deputy Secretary of Defense Memorandum, "Sensitive Technical Activities Oversight Committee (STAOC) Charter," November 21, 2020
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 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020
DoD Directive 5137.02, "Under Secretary of Defense for Research and Engineering (USD(R&E))," July 15, 2020
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," November 21, 2014, as amended
DoD Directive 5148.13, "Intelligence Oversight," April 26, 2017
DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," November 7, 2023
DoD Directive 7045.20, "Capability Portfolio Management," September 25, 2023
DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended
DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, 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 5205.11, "Management, Administration, and Oversight of DoD Special Access Programs," September 12, 2024
DoD Instruction 5530.03, "International Agreements," December 4, 2019
DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012, as amended
DoD Manual 5200.45, "Instructions for Developing Security Classification Guides," April 2, 2013, as amended
Executive Order 13526, "Classified National Security Information," December 29, 2009
National Security Directive 42, "National Policy for the Security of National Telecommunications and Information Systems," July 5, 1990
United States Code, Title 44