



Special Access Program (SAP) Stacks GLOSSARY

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

Term/Acronym

Definition

ACCESS

Access approval for a SAP is a separate and distinct action from national security access and eligibility determinations. If a SAPIA is not signed, SAP access will not be granted.

ACQUISITION

Acquisition SAPs are established to protect sensitive research, development, testing, and evaluation, modification, and procurement activities.

APPORTIONED

SAP or a section of SAP that is formally included in the IISTO process for Combatant Command use during deliberate planning, crisis action response, and operational employment.

BANNER

Banner Line; a display or listing at the top and bottom of a document page that conveys the highest classification level of information contained in the document/page and the most restrictive control markings applicable to the overall document/page.

CARVE OUT

A provision approved by the Secretary or Deputy Secretary of Defense that relieves DCSA of its National Industrial Security Program (NISP) obligation to perform industrial security oversight functions for a DoD SAP.

CERTIFIED TEMPEST TECHNICAL AUTHORITY

An experienced, technically qualified U.S. Government employee who has met established certification requirements in accordance with CNSS (NSTISSC)

approved criteria and has been appointed by a U.S. Government Department or Agency to fulfill CTTA responsibilities.

CODE WORD *A single word assigned to a SAP with a classified meaning (Confidential or higher), once activated by the appropriate authority, to emphasize the required degree of security and to safeguard information pertaining to SAPs.*

COMPLIANCE *Core Compliance Inspection; an inspection conducted at least once every 2 years, consisting of a self-inspection, core functional areas, and special emphasis items.*

CONTINUOUS EVALUATION
Continuous Evaluation (CE) is an ongoing screening process to review the background of an individual who is assigned to a sensitive position or has access to classified information or material.

CONTRIBUTE Materially
Material Contribution refers to a specific, measurable contribution by the individual sponsored for access to a Special Access Program.

DATA SPILL *Classified data is spilled either onto an unclassified information system or to an information system with a lower [or different] level of classification [or access]. [CNSSI 4009] Also referred to as data exfiltration – the unauthorized transfer of data from a system.*

DEBRIEF *The process of informing a person their need-to-know for access to SAP information is no longer required or has been terminated.*

DENIED *Denial of eligibility for access to National Security Information, an adjudicative decision that an individual is not eligible for access to classified information (United States Government (USG) Interagency Associated Terms). With regards to SAPs, a denial of SAP access does not mean inability of access to other classified information, but denial of national security eligibility would mean an inability to access SAP information by default.*

DEROGATORY *Derogatory Information; information that reflects on the integrity or character of an individual or circumstances that suggests that their ability to safeguard national security information may be impaired, that their access to classified or sensitive information clearly may not be in the best interest of national security, or that their activity may be in conflict with the personnel security standards or adjudicative guidelines.*

e-QIP *Electronic Questionnaires for Investigations Processing; a web-based automated system that was designed to facilitate the processing of standard investigative forms used when conducting background investigations for federal security, suitability, fitness, and credentialing purposes. e-QIP allows the user to electronically enter, update, and transmit their personal investigative data over a secure internet connection to a requesting agency.*

ENHANCEMENT *SAP is a classified program with enhanced safeguarding and access requirements to existing systems to provide equal or improved security features and safeguards.*

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

FSE *File Series Exception; an exception to the 25-year automatic declassification provisions of Executive Order 13526. SAPs established pursuant to DoD Directive 5205.07 have been granted the ability to classify information for up to 50 years.*

GPM *Government Program Manager; also known as a commander or a director. The GPM is responsible for the management of SAP(s).*

HVSACO *Handle Via Special Access Channels Only; a handling caveat used within SAP control channels rather than a classification level. It is used to identify classified or unclassified information that requires handling in SAP control channels due to its sensitivity when associated with a SAP(s). The term "SAP control channels" denotes secure and approved SAP communications systems, SAP facilities, or SAP-approved storage areas.*

LIFECYCLE *SAP lifecycle (establishment: a program is initially considered for SAP eligibility, management, and administration, is the day-to-day operation of the SAP, and the program undergoes inspections, audits, and internal control; apportionment: the phase in which the DoD Component and PSA SAPCOs nominate SAP capabilities to be apportioned into IJSTO when they are deemed to have operational capability; and disestablishment: includes ensuring the SAP's information and related SAPs are protected, a disestablishment plan is developed, and a debrief of personnel and a closeout inspection are conducted).*

LOCN *Letter of Compelling Need; a written description of an individual's unique skills or knowledge, the benefit the SAP will gain by accessing the individual, and why no other individual can fulfill or is readily available to fulfill that position.*

NICKNAME *Two separate unclassified words that are used in combination to represent a specific SAP or portion thereof.*

NTK *Need To Know; a criterion used in security procedures that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties. (JP 2-01.2)*

OVERSIGHT *The authority to monitor, review, inspect, investigate, analyze, and evaluate the management, operation, performance, and processes for DoD SAPs.*

PAR *Program Access Request; form required as part of the nomination process. Justification will be provided to address why access is required by establishing a need to know (NTK) and the nominated individual's material contribution to the SAP.*

POLYGRAPH *An instrument that: (1) records continuously, visually, permanently, and simultaneously changes in cardiovascular, respiratory, and electro dermal patterns as minimum instrumentation standards; and (2) is used, or the results of which are used, for rendering a diagnostic opinion regarding the honesty or dishonesty of an individual.*

PORTION *Portion Marking; using classification identifiers to independently mark sections, parts, or paragraphs as classified material. The classification of each portion depends solely upon the content of that portion. Portion markings shall be placed immediately preceding the material or data to remove any doubt as to the classification of a particular portion.*

PSO *Program Security Officer; responsible for the daily operation of the facility. Notifies the SAP Facility Accrediting Official (SAO) of any activity that affects the accreditation. PSOs may perform SAO functions when designated by the CA SAPCO.*

PSQ *Pre-Screening Security Questionnaire; a form that must be completed to initiate the SAP Nomination Process (SAPNP). It will be maintained in the appropriate SAP access management database or personnel security file. Additionally, this form must be revalidated or completed again annually.*

<https://www.dcsa.mil/mc/ctp/special/templates/>

QUAD CHART *A quad chart is a one-page document that is structured with four equal quadrants: a picture or graphic depiction of the program in the upper left, the SAP description in the lower left, status and issues in the upper right, and budget and schedule in the lower right. Assistance in developing a SAP quad chart is available from the CA SAPCO.*

REVOCAATION *Rescinding SAP access when a currently SAP-accessed individual is determined to be ineligible.*

SAO *SAP Facility Accrediting Official; a properly trained SAP facility accrediting official designated by the CA SAPCO to physically inspect and review and approve or disapprove physical security preconstruction plans for a Special Access Program Facility (SAPF), Temporary SAP Facility (T-SAPF), SAP Compartmented Area (SAPCA), and SAP Working Area (SAPWA) or SAP Temporary Secure Working Area (SAPTSPA) before accreditation.*

SAPCO *SAP Central Office; the office within a DoD Component or Office of the Secretary of Defense (OSD) Principal Staff Assistants (PSAs) that, when directed, executes,*

manages, administers, oversees, and maintains records on the SAPs for which it has been assigned by a cognizant authority (CA). Responsibilities may also include developing and implementing policies and procedures for oversight, management, execution, administration, SAP security, Information Assurance (IA), and records management of SAPs under their cognizance, as directed.

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

SAPIA *SAP Indoctrination Agreement; brief acknowledging the requirements for gaining access to SAP(s) and SAP-specific requirements.*

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

SPECIAL ACCESS PROGRAM

A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. Information to be protected within the SAP is identified by a Security Classification Guide (SCG).

SPO *SAP Personnel Security Official; an individual that has been trained and nominated to apply enhanced security procedures to determine personnel eligibility for access to DoD SAPs in accordance with this volume.*

SUPERIOR *The highest of the given possible ratings (Superior, Commendable, Satisfactory, Marginal, and Unsatisfactory) that a program may receive during the course of an inspection. Reserved for a contractor or government location that has consistently and fully implemented the security requirements in an effective*

fashion, resulting in a superior security posture compared with other contractor or government locations of similar size and complexity.

SUSPENSION *Suspension of Access; an action taken regarding a currently SAP-accessed individual as a result of certain personnel security conditions or questionable circumstances.*

TEMPLATE *In regards to SAPs; any one of a number of forms that are utilized as part of the administration of security within a program (e.g., SAP Training Record Template, Pre-Screening Security Questionnaire, PSQ Templates).*

<https://www.dcsa.mil/mc/ctp/special/templates/>

UMBRELLA *A SAP may also be referred to as an “umbrella” if the SAP has subordinate elements, referred to as compartments, sub-compartments, or projects.*

VIOLATION *A security violation is any knowing, willing, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information.*

WAIVED *A waived SAP is an unacknowledged SAP for which the SECDEF has waived applicable reporting in accordance with Reference (c) following a determination of adverse effect to national security. Also, it is an unacknowledged SAP that has more restrictive reporting and access controls than other unacknowledged SAPs.*

WAIVER *A decision that provides an approved exception to or deviation from a SAP security standard.*

ZDUCT *ZDUCT; Portion of duct comprised of two 90 degree angles in order to absorb sounds preventing it from leaving the SAP defined in IC Tech Spec – for ICD/ICS 705.*
