Chapter 8

SPECIAL ACCESS PROGRAMS

8-100 Policy

It is the policy of the Department of Defense to use the security classification categories and the applicable sections of E.O. 12958 and its implementing 1S00 Directives to limit access to classified information on a "need-to-know" basis only to those personnel who have been determined to meet requisite personnel security requirements. Further, it is DoD policy to rigorously apply the need-to-know principle in the normal course of controlling collateral classified information so that Special Access Program (SAP) controls will be used only when exceptional security measures are required based on threat and/or vulnerability (e.g. sensitivity or value of the information) associated with the SAP. Need-to-know principles shall also be applied within SAPS. In this context, SAPS maybe created or continued only on a specific finding that:

a. The vulnerability of, or threat to, the specific information to be protected is exceptional;

b. Normal criteria for determining access to the assigned level of classification are not sufficient to protect the information from unauthorized disclosure;

c. Careful consideration is given to: assessing the vulnerability, the sensitivity of the information to be protected, and the adequacy of needed safeguarding requirements; and/or

d. The establishment of the SAP is required by statute.

8-101 SAP Procedures

Unless exempted by the Secretary of Defense or Deputy Secretary of Defense, the DoD SAP Oversight Committee, (SAPOC), management structure and its working level Senior Review Group (SRG) shall be the forum for addressing the approval and disapproval for all DoD SAPS. In brief, the DoD utilizes a SAP Coordination Office (SAPCO), to support the SAPOC. The SAPOC is a matrix management organization that is made up of three OSD-level SAP Central Offices. The required approval documents shall be processed through the appropriate Unified Commands or respective component to the appropriate OSD-level SAP Central Office (i.e., Acquisition SAPS to Director, Special Programs, OUSD (A&T)); Operations and Support SAPS, Director, Special Programs, ODTUSD(P)PS, OUSD(P); and Intelligence SAPS, Director, Special Programs, OASD (C3I). The OSD-level SAP Central Office will "sponsor" the program for SAP approval and as apart of the SAPCO control it as it is processed through the SRG and SAPOC management structures to the Deputy Secretary of Defense, Chairman, SAPOC. In addition, the OSD-level SAP Central Offices must be advised of all non-DoD SAPS that have DoD participation (e.g., DoD personnel performing any program functions). SAPS that are NOT DoD SAPS, but which have active DoD support must be reported to one of the three cognizant OSD-level Central Offices. Specifically:

a. SAPS involving NATO classified information are based on international treaty requirements. DoD involvement with these SAPS must be reported to the Director, Special Programs, ODTUSD(P)PS, OUSD(P).

b. The policies and procedures for access to and dissemination of Restricted Data, (RD) and Critical Nuclear Weapon Design Information, (CNWDI) are contained in DoD Directive 5210.2. Any SAPS associated with RD and CNWDI must be reported to the Director, Special Programs, ODTUSD (P)PS, OUSD(P).

c. SAPS protecting foreign intelligence information under the cognizance of the Director of Central Intelligence (DCI) must be reported appropriately to either the Director, Special Programs, ODTUSD(P)PS, OUSD(P), or the Director, Special Programs, OASD(C3I), or to both. The National Security Act of 1947 and E.O. 12958 authorize the DCI to create SAPS pertaining to intelligence activities in accordance with Director of Central Intelligence Directive 3/29. The DCI is not authorized to create SAPS for military operational, strategic and tactical programs that are under the cognizance of the DoD.

d. When a DoD Component is involved with a SAP(s) or SAPS that involves one or more other DoD Component(s) or a non-DoD activity, DoD Components shall:

(1) Formalize or document the relationship in a written agreement (e.g., Memorandum of Agreement or Memorandum of Understanding) that specifies who has primary sponsorship of the program, and responsibility for obtaining SAP

approval.

(2) Provide to the appropriate OSD-level SAP Central Office notice that agreements have been executed with other DoD or non-DoD activities and make the details of the association available during oversight reviews as prescribed in DoD Directive 0-5205.7 and this Regulation.

e. Activities that do not involve acquisition or intelligence funds, and that protect purely military operations or the support thereof, are not reported or considered to be a DoD SAP per se. Rather, the activities within these programs are reported to the leadership and membership of Congress in the context of report of military operations as determined by the President and the Secretary of Defense.

f. SAPS involving participation by foreign governments shall be in compliance with DoD Directive 5230.11.

8-102 **Control and Administration**

a. SAPS shall be controlled and managed in accordance with DoD Directive 0-5205.7. The processes of the SAPOC, the SRG, the SAPCO, and the Special Access Program Policy Forum facilitate standardized and uniform security procedures and requirements. Specific responsibilities of the SAPOC, SRG, SAPCO, and SAP Policy Forum are defined in DoD Directive 0-5205.7.

b. The three OSD-level SAP Central Offices (Acquisition, Intelligence, and Operations and Support) have primary responsibility for (and authority over): (1) the types of activities conducted in the SAPS under their areas of cognizance; (2) endorsing or negotiating a change of the assigned category of a SAP, (3) collating, coordinating, and forwarding the SAPS annual reports; (4) conducting oversight reviews, as required; (5) reviewing and endorsing terminating or transitioning plans; and (6) ensuring SAPS do not duplicate or overlap other programs under its purview.

c. Each DoD Component shall establish a Component-level SAP Central Office to coordinate SAP requests for approval and otherwise "mirror" the activities of the three OSD-level SAP Central Offices. In addition to the specific responsibilities set forth in DoD Directive 0-5205.7, Component,-level SAP Central Offices shall maintain records of all SAPS and Prospective SAPS, (P-SAPS), under their cognizance to include approval documentation and, if appropriate, revalidation documentation. Records shall be retained for the life of the SAP and for 12 months after termination of the program.

d. In accordance with DoD Directive 5010.38 and Office of Management and Budget Circular A-123, the DoD Management Control Program (MCP) will be implemented within all SAPS. To ensure adequate implementation, DoD Components are required to have MCP coordinators within special access channels to:

(1) Provide guidance, training, and oversight on the MCP to SAP managers;

(2) Serve as the central point to which all SAP deficiencies (of a classified nature) that are identified through the MCP are reported; and

(3) Establish formal follow-up systems to ensure that SAP managers schedule corrective actions for all reported deficiencies to include monitoring deficiencies until resolved. Each Component will prepare an annex on SAPs to their annual statements of assurance to the Secretary of Defense or assert in their annual statement that no material weaknesses were reported within their SAPS. In either case, statements will be classified, if required, and will be sanitized from all special access program specific information. Reports will be reviewed by Component-level SAP Central Offices prior to forwarding outside SAP channels.

e. Unless specifically exempted by the SAPCO, SAP contract administration services shall be delegated to the Defense Contract Management Command's (DCMC) dedicated cadre of personnel. Also, the DCMC shall utilize the dedicated cadre of personnel of the Defense Contract Audit Agency for audit services, unless specifically exempted.

8-103 Establishment of DoD SAPS

a. In accordance with E.O. 12958, within the Department of Defense, only the Secretary of Defense or Deputy Secretary of Defense may create a SAP. The DoD Components proposing the establishment of SAPS shall evaluate and process proposals in accordance with the procedures in this Regulation, DoD Directive 0-5205.7 and other implementing directives. DoD Components are responsible for ensuring that Unified Combatant Commands are appropriately briefed and consulted during the development process. A SAP may not be initiated until the defense committees of Congress are notified of the program and a period of 30 days elapses after such notification is received.

b. The military Departments SAP Central Offices

or OSD-level SAP Central Offices may authorize a Prospective SAP (P-SAP). Upon authorization, enhanced security measures (i.e., SAP controls) may be applied to a P-SAP for up to 6 months. The program must be terminated if not submitted to SAPOC process after 6 months or formally extended by the Director, SAPCO. Except for minor administrative security operations and maintenance ("O&M") funds needed to maintain security, no direct funding may be expended on any P-SAP without the required notifications to Congress. Transitional funds for associated efforts in some instances are authorized where direct funding is not applicable. In all cases, the Director or Deputy Director SAPCO must be notified of the establishment or termination of P-SAPS through the appropriate OSD-level SAP Central office.

c. Before initiating a SAP, notifying Congress, or expending funds on a SAP, the DoD Components shall forward a request for approval of the SAP and relevant funding documentation to the Deputy Secretary of Defense through the appropriate OSD-level SAP Central Office for processing through SAPOC management structure. The Director, Special Programs, ODTUSD(P)PS, OUSD(P) shall review the security requirements on behalf of the SAPOC.

d. The request package shall include the following:

(1) Identification of the responsible office or DoD Component, including office designation and symbols. Identification of the Component-level SAP Central Office official who is the point of contact for the SAP (full name, position or title, mailing address, and telephone number).

(2) The unclassified nickname(s) and, if used, the classified code word(s) for the SAP and its subelements or subcompartments. NOTE: All DoD SAPs shall have an unclassified nickname assigned and utilized.

(3) The designation of the SAP's category as an Acquisition, Intelligence, or Operations and Support SAP and whether the SAP is unacknowledged or acknowledged. The type of funding being used and the associated recommendation of the sponsoring DoD Component and subsequent Deputy Secretary of Defense approval determines the category. The DoD SRG may make appropriate recommendations for a change in a SAP category as a part of the annual review process.

(4) The relationship, if any, to other DoD and/or non-DoD SAPS, to include the identification of existing agreements, memorandums of understanding, or similar arrangements that pertain to the proposed DoD SAP.

(5) Justification for establishing the Program as a SAP, including the reasons why normal management and safeguarding procedures for classified information are not sufficient, a description of the threat that can exploit identified vulnerabilities, and how the additional special security procedures will compensate for or mitigate those vulnerabilities.

(6) Budgetary information in the format contained in Appendix I.

(7) The total estimated number of persons who will require access to the SAP during the first year. Separate the total into the following categories: sponsoring DoD Component; other DoD Components and activities; other Government Agencies; contractors; and elsewhere in the private sector.

(8) A program security classification guide, a program security policy and procedures plan, and an operational policy. The security policy and procedures plan shall include personnel security, physical security, automated information systems security, etc., and proposed counterintelligence and operations security requirements and support. These documents should embody any "risk management" concepts that are applied.

(9) If contractors area part of the program, a statement that a DD Form 254, *Contract Security Classification Specification*, has been issued to contractors participating in the program. The statement will include identification of which elements and/or overprinted elements of DoD 5220.22-M-Sup. 1, *National Industrial Security Program, Operating Manual Supplement*, (NISPOMSUP) apply to the SAP.

(10) If applicable, a request and justification for waiver to any specific criteria specified by this Regulation and, if applicable, the DoD 5220.22-M-Sup. 1.

(11) If applicable, a justification for those functions that will be performed by the SAP that are normally performed by centralized organizations or specialized cadres of personnel who are dedicated to performing SAP-related functions within those organizations (e.g. contract administration services, contract payment, travel reimbursement). Specifically, if contracting is part of the SAP, a

request must be made to relieve or "carve-out" the Defense Investigative Service (DIS), see Carve-Out Contracts, paragraph 8-103e., below. In some instances where the normal organizations are not used, it must be fully explained how the required tasks, security and other unique tasks, will be performed for the SAP.

(12) If applicable, a request and justification to waive the SAP reporting requirements specified by Section 119(e), title 10, United States Code.

(13) Identification of those members of Congress and Congressional staffs who have knowledge of the SAP in its proposed configuration or in some earlier form.

(14) Proposed Congressional notification letters to the chairperson and ranking minority member of: the Committee on National Security, House of Representatives, the Committee on Armed Services, United States Senate, the Subcommittee on Defense, Committee on Appropriations, House of Representatives, and the Subcommittee on Defense, Committee on Appropriations, United States Senate. See format in Appendix I.

(15) The endorsement by the head of the sponsoring DoD Component, and a request for approval by the Deputy Secretary of Defense forwarded through the appropriate OSD-level SAP Central Office having program cognizance, to the Director, SAPCO.

(16) The date that the program is scheduled to be established and any associated constraining time frames.

e. Carve-Out Contracts

(1) The use of contracts that relieve DoD organizations of their established contract related responsibilities must be fully explained and justified. If the SAP will perform the functions of review and/or inspection, the responsibilities of the Cognizant Security Office(s), or investigative functions, a request must be made to relieve DIS from their responsibilities under the National Industrial Security Program, and the practice must be identified as a "carve-out". Carve-outs are prohibited unless:

(a) The contract in question supports a SAP that has been approved by the SAPOC.

(b) Mere knowledge of the existence of a particular contract or its association with the SAP is classified and designated as SAP protected information; and

(c) The carve-out status for the SAP on its contract was approved as a part of the DoD SAPOC process.

(2) The DD Form 254, classified if necessary, shall be used to document a carve-out contract. The DD Form 254 shall identify specific areas, or locations within a contractor's facility that define the extent of the carve-out, (e.g., a safe, a room, or a particular building). It will also identify the CSO and CSA. The Component-level SAP Central Office shall provide a copy of each DD Form 254 to the appropriate DIS cognizant security office and, if applicable, to the Director, Defense Contract Audit Agency (DCAA). In exceptional instances the OSD-level SAP Central Office may, with concurrence of the Director, Special Programs, ODTUSD(P), OUSD(P) convey appropriate written notification defining the extent of the carve-out directly to the Director, DIS, and if applicable to the Director, DCAA.

(3) Approved carve-out contracts shall be afforded the support from the sponsoring Component-level SAP Central Office for the protection of the classified information involved. The support shall be provided through a system of controls that includes, but is not limited to, the following elements:

(a) Designate a central office of record and an official designated to be the single point of contact for SAP security planning, control, and administration. These security plans shall be submitted to the Director, Special Programs, ODTUSD(P), OUSD(P) for review and endorsement as a part of the SAPOC approval process.

(b) A Written Security Plan. The plan will include, if applicable, how security will be accomplished for contractors. An overprinted DoD 5220.22-M-Sup. 1 will be provided if contracts area part of the SAP. Oral changes or deviations from the written plan are prohibited except in critical situations. These changes will be documented as soon as practicable after the fact.

(c) Security Review Procedures. The procedures will ensure that fully qualified government professional security personnel of the sponsoring DoD Component perform security reviews at each contractor's facility with the frequency, generally, prescribed by of DoD 5220.22-M-Sup. 1. NOTE: Reviews for cause or supporting visits may be as frequently as warranted by "risk management" principles.

(d) Specialized procedures to be followed for developing and implementing contracts for unacknowledged SAPS.

f. Nicknames and Code words

(1) Each DoD SAP shall be assigned an unclassified nickname. Classified code words may also be assigned to SAPS but are optional. Military Departments and DoD Components shall develop a system to assign and administer nicknames and code words for SAPS for their Departments. The DoD Components other than the Military Departments may request nicknames and code words for SAPS from the appropriate OSD-level SAP Central Office, (See Chairman of the Joint Chiefs of Staff Manual CJCSM 3150.29 for more information.)

(2) Non-DoD originated nicknames and code words used by DoD Components participating in non-DoD SAPS shall be registered with the appropriate OSD-level SAP Central Office and the JCS central registry to prevent confusion with DoD-originated words. (NOTE: Some non-DoD Executive Branch organizations do not observe the same two word and/or nickname and one word and/or code word policy as does the DoD.)

(3) Within the Department of Defense, a nickname is a combination of two separate unclassified words. Do not use combination of words including "project," "exercise," or "operation" or words that may be used correctly either as a single word or as two words, such as moon-light. Do not use exotic words, trite expressions, or well-know commercial trademarks. A nickname should not:

(a) Express a bias inconsistent with traditional American ideals or foreign policy.

(b) Convey connotations offensive to good taste or derogatory to a particular group, sect, or creed, or

(c) Convey connotations offensive to our allies or other nations, or

(d) Be discussed on an unclassified communication net unless all aspects including organizational associations are completely unclassified. (NOTE: The use of STU III while discussing or mentioning nicknames is very strongly encouraged.)

(4) Within the Department of Defense, a code word is a single word assigned a classified meaning by appropriate authority. It is classified as CONFIDENTIAL or higher. A code word shall not be assigned to test, drill, budget identifiers, or exercise activities. The using Component shall assign to a code word a specific meaning classified SECRET or CONFIDENTIAL. Code words shall not be used to cover unclassified meanings. TOP SECRET code words may be issued only with Director, Special Programs, ODTUSD(P), OUSD(P) approval or by the DoD component in coordination with the Director, Special Programs, ODTUSD(P), OUSD(P). The assigned meaning need not in all cases be classified as high as the overall classification assigned to the program or operation. Code words shall not suggest the nature of its meaning. It shall not be used repeatedly for similar purposes; that is, if the initial phase is designated "Meaning," succeeding phases should not be designated "Meaning II" and "Meaning III," but should have different code words. Each DoD Component shall establish policies and procedures for the control and assignment of classified meaning to code words. No code word may be discussed on an unclassified communication net or telephone.

8-104 Reviews of SAPS

a. To facilitate management's stewardship over SAPS, each DoD SAP shall be reviewed annually by the DoD Component responsible for initiation and sponsorship of the program, in coordination with appropriate Unified Combatant Commands. These reviews shall include annual regularly scheduled audits by security, contract administration, and audit organizations. Written records of these reviews and audits shall be maintained for the lifetime of the SAP and for 12 months following its termination. These records shall be available for evaluation during the OSD-level SAP Central Office program reviews.

b. As part of the annual reporting and revalidation of all DoD SAPS, the DoD Components shall ensure that these programs continue to be reviewed by qualified legal counsel for compliance with applicable laws, executive orders, and regulations.

c. The OSD-level SAP Central Offices shall conduct oversight reviews, as required, to determine compliance with DoD Directive 0-5205.7 and this Regulation, to specifically include verification of the conduct of Component-level annual security reviews.

d. The ODTUSD(P)PS, OUSD (P), shall conduct appropriate annual oversight reviews of each SAP Central Office and, as deemed necessary, on-sight program security reviews at Government and contractor locations.

e. The Inspector General of the Department of Defense shall conduct oversight of DoD SAPS, pursuant to statutory authority.

f. Oversight, review, and SAP support activities shall accomplish their functions using small cadres of specially cleared and qualified personnel, sufficient in size to address the SAP workload. The cadre's primary responsibility is to support SAPS.

8-105 Annual Reports and Revalidation

a. Section 119 of title 10, United States Code requires that not later than March 1 of each year, the Secretary of Defense shall report all DoD SAPS to Congress. These annual reports also serve as the vehicle for revalidation and approval for continuation of all DoD SAPS by the Deputy Secretary of Defense. Any SAP not granted approval to continue shall be terminated.

b. Not later than December 15 of each year, the Component-level SAP Central Office shall submit reports for the Deputy Secretary of Defense on all SAPS under their sponsorship. Since the President's budget may not be available by that date, provide the best estimate as a part of the report with actual budget numbers being provided as soon as they are available.

c. For each SAP sponsored, the DoD Components shall prepare separate reports and "Quad Charts" in the format shown in Appendix I in both MS Word and hard copy. The reports and "Quad Charts" shall be forwarded to the appropriate Component-level SAP Central Office for processing. All information elements may not apply to all SAPS; however, as a minimum, each report must include:

(1) Justification for continuation of the Program as a SAP;

(2) If applicable, justification for continuation of the exclusion of the SAP from the review requirements of the National Industrial Security Program (i.e., continuation of carve-out status); and,

(3) If applicable, justification for continuation of status as a Waived SAP under Section 119(e), title 10, United States Code.

d. Components' submissions shall also include a certification that there are no unreported SAPS or SAP-like programs, or an explanation for any programs not included in the report. Any SAP being terminated or unfunded must be clear] y identified.

e. The Component-level SAP Central Office shall aggregate reports by category of SAP (acquisition, intelligence, and operations and' support), and shall forward them to the appropriate OSD-level SAP Central Office. The OSD-level SAP Central Offices shall collate and forward the reports to the Director, SAPCO for Deputy Secretary of Defense action. After action by the Deputy Secretary of Defense, the reports will be returned to the SAPCO.

f. The SAPCO notifies Congress of the Deputy Secretary of Defense's decisions and then returns the reports to the OSD-level SAP Central Offices for distribution and action.

g. SAPS that are approved by the Deputy Secretary of Defense as Waived SAPS under Section 119(e), title 10, United States Code, shall be reported on a case-by-case basis to appropriate members of Congress, in accordance with applicable law, with specific direction from the Secretary or Deputy Secretary of Defense.

8-106 Interim Reporta

The Component-level SAP Central Office shall immediately notify (through the OSD-level SAP Central Office) the Director, SAPCO, when there is a SAP or subcompartment nickname or code word change. Any additions, deletions, or corrections to the annual report should be reported as they occur during the year to include subcompartments. The interim report shall contain, at a minimum, the nickname affected, effective date of the change, and information that has been changed from the previous report.

8-107 Changes **in Classification**

a. DoD Components intending to downgrade the classification of a SAP, transition from unacknowledged to acknowledged, remove enhanced controls from a SAP and/or move the program to a collateral security level, declassify a program, or make a public announcement concerning any of these activities, shall prepare letters of notification to the appropriate Congressional Committees in accordance with the format in Appendix I. This requirement also applies to significant subelements or subcompartments of SAPS that could potentially be of interest to the Congress (i.e., generally this will necessitate reporting acquisition SAP subelements and most major subelements of intelligence, and operation and support SAPS, and when sub-compartments are not significant enough to be separately reported, these instances will be coordinated with the appropriate OSD SAP Central Office). This reporting requirement also applies to programmatic information

that is being made public. The DoD Components shall forward these letters through the appropriate Component-level, OSD-level SAP Central Offices, and the Director, SAPCO, for processing to the Deputy Secretary of Defense. The letter shall contain a description of the proposed change, the reasons for the proposed change, and notice of any public announcement planned to be made about to the proposed change.

b. After approval and signature by the Deputy Secretary of Defense, notification letters shall be returned to the SAPCO for delivery to Congress by the DoDC component or the SAPCO. No action relative to the change in classification or enhanced security measures (i.e., removal from or change SAP status) of the SAP shall be taken or any announcement made sooner than 14 days after the letters have been delivered to the appropriate committees in Congress, unless authorized pursuant to statute by the Deputy Secretary of Defense.

8-108 **Termination and Transitioning of SAPS**

a. SAPS shall be carefully but promptly terminated or transitioned to collateral security programs when there is no longer a need for the enhanced security protection.

b. DoD sponsoring Components shall prepare SAP termination plans (i.e., a Plan of Action and Milestones, how the "de-sapped" program will comply with the Acquisition System Protection requirements). The plan will outline the security measures that will be followed when terminating or transitioning a SAP. The plan shall identify information that will remain classified and as appropriate, the OPSEC measures designed to protect any sensitive unclassified indicators, or methods associated with the SAP. A time and/or event phased (as deemed most appropriate) Security Classification Guide shall be included in the plan. The plan shall take into consideration continuing collateral security requirements in all functional areas to include the technical aspects, funding, contracting operations, legal, logistics, training, and administrative requirements. The DoD Components shall forward the termination and/or transitioning plan to the appropriate OSD-level SAP Central Office for review and endorsement.

c. In all cases, the notification procedures set forth in subsection 8-107 above, shall be followed before actual termination or transition of a SAP is effected.