Department of Defense

INSTRUCTION

NUMBER 5205.11
February 6, 2013
Incorporating Change 2, February 4, 2020

DoD SAPCO

SUBJECT: Management, Administration, and Oversight of DoD Special Access Programs (SAPs)

References: See Enclosure 1

1. PURPOSE. This instruction reissues DoD Instruction (DoDI) O-5205.11 (Reference (a)) in accordance with the authority in DoD Directive (DoDD) 5205.07 (Reference (b)) to establish policy and implement the policy established in Reference (b), assign responsibilities, and to update and prescribe procedures for the management, administration, and oversight of all DoD SAPs.

2. APPLICABILITY. This instruction:

a. Applies to:

(1) OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff (JS), the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the DoD (referred to collectively in this instruction as the "DoD Components").

(2) All DoD Component contractors and consultants that require access to DoD SAPs pursuant to the terms and conditions of the contract.

(3) 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.

b. Does not apply to the management and oversight of DoD activities using alternate compensatory control measures (ACCMs). ACCMs are not SAPs. Guidance for ACCMs is contained in Volume 3 of DoD Manual 5200.01 (Reference (c)).

3. POLICY. It is DoD policy that:

a. DoD SAPs must be established and maintained only when absolutely necessary to protect the Nation's most sensitive capabilities; information; technologies; operations; and research, development, test and evaluation; or when required by statute pursuant to Reference (b). Establishment must be consistent with Executive Order (E.O.) 13526 (Reference (d)).

b. DoD Components must conduct all DoD SAPs in accordance with Reference (b) and this instruction.

c. DoD SAPs must be protected at all times consistent with their classification and sensitivity.

d. All DoD SAPs must be assigned an unclassified nickname generated in accordance with Chairman of the Joint Chiefs of Staff Manual 3150.29D (Reference (e)) to facilitate program protection and administration and Congressional reporting requirements. The cognizant authority (CA) Special Access Program Central Office (SAPCO) will determine whether a classified codeword will also be used. Unclassified nicknames will be used in the annual SAP report to Congress.

e. Only the SAPCO Directors of the Army, Navy, Air Force, JS, Office of the Under Secretary of Defense for Policy (USD(P)), Office of the Under Secretary of Defense for Intelligence and Security (USD(I)), and Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) will initiate the process for establishment of prospective DoD SAPs (PSAPs) in accordance with Reference (b).

f. In accordance with DoDI 5220.22 (Reference (f)), the Defense Security Service (DSS) has National Industrial Security Program (NISP) cognizant security authority (CSA) for all DoD unless the CSA for a specific SAP has been specifically assigned to another CSA, referred to in this instruction as "carved out," by the Secretary of Defense (SecDef) or Deputy Secretary of Defense (DepSecDef).

g. DoD employees who meet personnel access or prerequisite eligibility criteria and have assigned legal, fiscal, audit, investigative, operational, or statutory oversight or regulatory duties for DoD SAPs must be deemed to have need to know (NTK) for access and will be granted effective and sufficient access to those programs when determined necessary by an access approval authority (AAA) to meet their responsibilities.

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES

a. The SAP governance structure (consisting of the SAP Oversight Committee (SAPOC), the Senior Review Group (SRG), and the SAP Senior Working Group (SSWG)) will advise and

assist the SecDef and DepSecDef in the management, administration, and oversight of DoD SAPs. The membership and functions of the SAP governance structure are described in Enclosure 3.

b. Access to a SAP will be strictly limited to the minimum number of personnel necessary for execution of the program. Granting access to a SAP will be based solely upon a determination that the individual has a valid NTK, has the requisite security clearance, meets approved personnel prerequisites, and will clearly and materially contribute to the execution or oversight of the program. Eligibility prerequisite procedures are described in Enclosure 4.

c. DoD SAPs may include subordinate activities identified as, in descending order, compartments, sub-compartments, and projects when approved and reported as specified in this instruction. The SAP hierarchy of activities is discussed in Enclosure 5.

d. Required SAP life-cycle management procedures are provided in Enclosure 6.

e. Required program record files are addressed in Enclosure 7.

f. SAP procedures for JS and Combatant Commands are in Enclosure 8.

g. Procedures for foreign disclosure are in Enclosure 9.

6. INFORMATION COLLECTION REQUIREMENTS. The SAP report, referred to in paragraphs 1b, 4a, 5i, and 5q of Enclosure 2 and paragraphs 2e, 2f, and 2g of Enclosure 6 of this instruction, is submitted to Congress in accordance with section 119 of Title 10, United States Code (Reference (g)) and is coordinated with the Assistant Secretary of Defense for Legislative Affairs in accordance with the procedures in DoDI 5545.02 (Reference (h)).

7. RELEASABILITY. **Cleared for public release.** This instruction is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

8. SUMMARY OF CHANGE 2. This change reassigns the office of primary responsibility for this instruction to the DoD Special Access Programs Central Office in accordance with the August 3, 2018 Deputy Secretary of Defense Memorandum (Reference (i)) and updates references.

9. EFFECTIVE DATE. This instruction is effective February 6, 2013.

Ashton B. Carter
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities
3. SAP Governance Structure
4. SAP Access Prerequisites
5. SAP Hierarchy
6. SAP Life-Cycle Management
7. Program Record Files
8. JS and Combatant Command SAP Procedures
9. Foreign Disclosure Procedures

Glossary

TABLE OF CONTENTS

FIGURES

ENCLOSURE 1

REFERENCES

(a) DoD Instruction O-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," July 1, 1997 (hereby cancelled)
(b) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended
(c) DoD Manual 5200.01, "DoD Information Security Program," February 24, 2012, as amended
(d) Executive Order 13526, "Classified National Security Information," December 29, 2009
(e) Chairman of the Joint Chiefs of Staff Manual 3150.29D, "Code Word, Nickname, and Exercise Terms (NICKA) System," October 15, 2010
(f) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended
(g) Section 119 of Title 10, United States Code
(h) DoD Instruction 5545.02, "DoD Policy for Congressional Authorization and Appropriations Reporting Requirements," December 19, 2008
(i) Deputy Secretary of Defense Memorandum, "Restoring Special Access Program Responsibilities to the Deputy Secretary of Defense," August 3, 2018
(j) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992
(k) DoD Manual 3305.13, "DoD Security Accreditation and Certification," March 14, 2011, as amended
(l) DoD Instruction 5230.28, "Policy for Low Observable (LO) and Counter Low Observable (CLO) Programs (U)," May 26, 2005, as amended
(m) DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons," December 1982, as amended
(n) DoD Directive S-5210.36, "Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government (U)," November 6, 2008, as amended
(o) DoD Instruction 5210.91, "Polygraph and Credibility Assessment (PCA) Procedures," August 12, 2010, as amended
(p) Executive Order 12968, "Access to Classified Information," August 2, 1995
(q) Office of Management and Budget Policy Memorandum, "Reciprocal Recognition of Existing Personnel Security Clearances," July 17, 2006
(r) DoD Instruction 5200.39, "Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)," May 28, 2015, as amended
(s) DoD 7000.14-R, Volumes 2A and 2B, "Department of Defense Financial Management Regulations (FMRs): Budget Formulation and Presentation," current edition
(t) DoD Directive 5205.02E, "DoD Operations Security (OPSEC) Program," June 20, 2012, as amended
(u) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

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

[1] NDP-1 is a controlled document provided by the NDP Committee to Principal and Designated Disclosure Authorities on a need-to-know basis from the Office of the Director for International Security Programs, OUSD(P). This document is classified SECRET.

ENCLOSURE 2

RESPONSIBILITIES

1. DIRECTOR, DoD SAPCO. Under the authority, direction, and control of the DepSecDef, and in addition to the responsibilities in Reference (b), the Director, DoD SAPCO:

a. Implements procedures for sharing DoD SAPs with foreign entities consistent with DoDD 5230.11 (Reference (j)). Facilitates and maintains MOAs and memorandums of understanding (MOUs) for foreign involvement with DoD SAPs and coordinate with the appropriate oversight authorities (OAs) and CAs.

b. Annually prepares the SAP report to Congress for DepSecDef approval in accordance with Reference (g)).

c. Provides administrative and management support to SAP congressional hearings and prepare and coordinate responses to congressional inquiries.

d. Serves as CA for SAP studies, portfolios, and associated billet structures involving DoD SAPs, exclusive of Service-initiated study efforts internal to the Military Departments.

e. Provides administrative and management support to OSD-level Executive Committees (EXCOMs).

f. Serves as the CA SAPCO for DoD Components not supported by an existing SAPCO and executes DoD SAPs or provides support functions, as specified in section 5 of this enclosure.

g. Notifies all DoD Component SAPCOs of suspensions, revocations, and reinstatements of SAP access.

h. Participates in DoD efforts to resolve security, technology transfer, and export issues; supports the Committee on Foreign Investment in the United States (CFIUS) and the foreign ownership, control, and influence certification process.

i. In coordination with the DoD Chief Information Officer (DoD CIO), establishes and administers governance and risk management policies to develop enterprise SAP information technology (IT) strategy, telecommunications infrastructure policy, SAP network IT requirements, and network and systems funding oversight policy.

j. Maintains and resources a secure network capability to facilitate exchange of selected information between DoD Components in support of SAP enterprise oversight and governance.

k. Establishes policies and applicable procedures to satisfy reporting requirements for DSS carve-outs, CFIUS, and treaty matters. Provides DSS confirmation of SAP facilities where the DSS has been carved out of security oversight functions.

l. Unless constrained by higher authority, coordinates with the OA and CA prior to taking action on any significant issues of a security nature that may adversely impact SAPs.

m. Establishes the criteria for annual reviews of waived DoD SAPs by the SSWG and SRG.

n. Oversees the Special Program Security Certification (SPSC). Appoints the SPSC lead component in accordance with DoD Manual 3305.13 (Reference (k)).

o. In accordance with Reference (c), notifies the Director of Security, OUSD(I), of security violations and significant security incidents involving SAP information.

2. DIRECTOR, USD(AT&L) SAPCO. Under the authority, direction, and control of the USD(AT&L), the Director, DoD SAPCO may serve as the Director, USD(AT&L) SAPCO. In addition to the responsibilities in section 5 of this enclosure, the Director, USD(AT&L) SAPCO:

a. Provides management oversight of the National Assessment Group.

b. Serves as:

(1) The Co-Chair of the SAP Acquisition Overarching Initiative with the OUSD(AT&L) Senior Official(s) appointed by USD(AT&L) to review selected acquisition SAPs on an annual basis.

(2) The Executive Secretary for Special Access Defense Acquisition Board reviews.

(3) The Director of Low Observable Technology, including serving as Executive Secretary of the Low Observable/Counter Low Observable (LO/CLO) EXCOM and Chair of the LO/CLO Tri-Service Committee, as detailed in DoDI 5230.28 (Reference (l)).

c. Provides the Director, Operational Test and Evaluation an updated copy of the congressional report on acquisition SAPs on a quarterly basis or more frequently, if circumstances dictate.

3. DIRECTOR, USD(P) SAPCO. Under the authority, direction, and control of the USD(P), in coordination with the DoD SAPCO, and in addition to the responsibilities in section 5 of this enclosure, the Director, USD(P) SAPCO:

a. Provides management and oversight to the OSD Special Technical Operations cell, which will address required SAP-related actions between OSD and the Integrated Joint Special Technical Operations (IJSTO) process.

b. Provides guidance and direction for sensitive DoD tests, to include SAP capabilities and technologies, and coordinates the DoD staff review and DepSecDef approval of these sensitive tests.

c. Provides support to the Special Assistant for Compartmented Activities.

4. DIRECTOR, USD(I) SAPCO. Under the authority, direction, and control of the USD(I), in coordination with the DoD SAPCO, and in addition to the responsibilities in section 5 of this enclosure, the Director, USD(I) SAPCO:

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 Coordination Office (CAPCO) Oversight Committee for all issues relevant to the DNI's Controlled Access Program Oversight Committee (CAPOC).

c. Serves as the SAPCO for the Office of the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)).

d. Deconflicts with CAPCO the names and abbreviations for DoD's SAPs and DNI's CAPs.

5. DIRECTORS OF THE DoD COMPONENT SAPCOs AND DIRECTORS OF THE PRINCIPAL STAFF ASSISTANT (PSA) SAPCOs WITH CA AND OA OVER DoD SAPs. Under the authority, direction, and control of their respective DoD Component heads and PSAs, the Directors of the DoD Component SAPCOs and Directors of the PSA SAPCOs with CA and OA over DoD SAPs:

a. Fulfill responsibilities, when assigned by the DoD Component head, as stated in Reference (b).

b. Immediately inform the DoD SAPCO of any significant issue of a security nature. Additionally, for issues of a criminal nature, notify the appropriately accessed representatives of the cognizant Defense Criminal Investigative Organization (DCIO).

c. Notify the DoD SAPCO of suspensions, revocations, and reinstatements of SAP access of personnel.

d. Facilitate secure exchange of selected information between DoD Components in support of SAP enterprise governance in accordance with paragraph 1.j. of this enclosure.

e. Utilize, where possible, SAP network and system capabilities identified by the DoD SAPCO as authoritative in support of SAP governance. Notify the DoD SAPCO, in writing, of requirements that preclude use of enterprise administrative network and system capabilities.

f. Review and make recommendations about the international security portions of DoD SAPs and related program information and capabilities in accordance with Enclosure 10.

g. Ensure appropriate review and compliance with DoD 5240.1-R (Reference (m)) for all intelligence SAPs.

h. Make SAP access eligibility decisions.

i. Participate in the SAP governance structure as described in Enclosure 3.

j. As part of the annual reporting and revalidation, ensure all DoD SAP annual reports are reviewed by legal counsel for compliance with applicable laws, E.O.s, regulations, and DoD policies.

k. Provide SAP security support for EXCOMs under their cognizance.

l. In accordance with Reference (b), submit the following actions through the Director, DoD SAPCO, to the DepSecDef:

(1) Proposals to establish or disestablish DoD SAPs.

(2) Requests for approval of proposed SAP types, categories, and classifications.

(3) Designation of and changes to the OA and CA.

(4) Removal of DoD programs from special access controls.

(5) Apportionment and deapportionment of DoD SAPs into and out of IJSTO.

(6) Alterations in the scope, category, or type of a SAP.

(7) Requests for the use of DoD resources to support non-DoD SAPs except for those approved under DoDD S-5210.36 (Reference (n)).

(8) Foreign disclosure actions (see Enclosure 10).

m. Nominate SAP capabilities for apportionment into IJSTO no later than 18 months prior to planned initial operational capability (IOC) or sooner if they have been tested and determined to be operationally effective. Waiver from this requirement rests with the SRG acting for the DepSecDef.

n. In accordance with Reference (f), make national interest determinations (NIDs).

o. Appoint a member to serve on the Special Access Program Policy Working Group.

p. Approve or disapprove the establishment or disestablishment of compartments, sub-compartments, and projects. Notify the DoD SAPCO of the establishment of compartments, sub-compartments, and projects. Summarize all compartment, sub-compartment, and project activity in the SAP annual report. In addition, the program hierarchy structure for each SAP

program included in the SAP annual report to Congress must be clearly defined, and that structure must be linked to the budget request. The Component levels of each program's structure is to be clearly displayed in the annual report to provide a stronger linkage between program activities, and requested program funding. The structure must be consistent both across DoD and within a Component's portfolio.

q. Collaborate with DoD Component records management programs in accordance with applicable directives and instructions to develop records disposition schedules related to the established DoD SAPs, compartments, sub-compartments, and projects.

r. Submit to the DoD SAPCO as part of the SAP annual report a consolidated summary of actions taken in support of the SAP files series exemption and records declassification.

s. Ensure DoD Government and contractor personnel accessed to DoD SAPs are aware of the requirement to bring all available information regarding any scheduled or proposed legal proceeding that involves the potential disclosure, use, or discussion of SAP material to the attention of the CA SAPCO and DoD SAPCO within 48 hours of learning of the proceeding.

ENCLOSURE 3

SAP GOVERNANCE STRUCTURE

1. GENERAL. The SAP governance structure comprises the SAPOC, SRG, and SSWG.

2. SAPOC. The SAPOC functions as the SAP governance, management, and oversight committee identified in Reference (b) and will advise and assist the SecDef and DepSecDef in discharging their responsibilities.

a. Membership. As set forth in Reference (b), members of the SAPOC are:

(1) Chair. The DepSecDef.

(2) Vice-Chair. The USD(AT&L).

(3) Executive Secretary. The Director, DoD SAPCO.

(4) General Membership

(a) USD(P).

(b) Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (USD(C)/CFO).

(c) USD(I).

(d) Under Secretary of Defense for Personnel and Readiness.

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

(f) DoD CIO.

(g) General Counsel of the Department of Defense (GC, DoD).

(h) Director, Cost Assessment and Program Evaluation (DCAPE).

(i) Under Secretaries for the Departments of the Army, the Navy, and the Air Force.

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

(k) Vice Chief of Naval Operations.

(l) Assistant Commandant of the Marine Corps.

b. Primary Functions. The SAPOC convenes at the direction of the DepSecDef to:

(1) Review issues referred by the SRG for which there is not a unanimous agreement.

(2) Ensure the war-fighting capability needs of the Combatant Commands and the requirement for an integrated joint force are reflected in programmatic and budgetary considerations for all DoD SAPs.

(3) Conduct an annual review and validation of SAP reports sent to the Congressional defense and intelligence committees.

3. SRG. The SRG is the principal working-level body executing the governance process and performing oversight and management of DoD SAPs. Unanimous recommendations of the SRG may be forwarded directly to the DepSecDef for decision.

a. Membership. Members of the SRG are:

(1) Chair. The Principal Deputy Under Secretary of Defense for AT&L.

(2) Vice Chair. The Director, DoD SAPCO.

(3) Executive Secretary. The Deputy Director, DoD SAPCO.

(4) General Membership. The SRG comprises the primary or alternate members, designated in writing by each SAPOC member. Only designated SRG members have voting rights within this body; however, in the case of the Army, Navy, and Air Force, only one individual will represent their respective Under Secretary and Vice Chief of Staff (one vote per Military Department). Additional appropriately cleared personnel may attend if approved by the SRG Chair.

b. Primary Functions. The SRG:

(1) Convenes at the direction of the DepSecDef to:

(a) Review proposals to establish or disestablish SAPs.

(b) Designate the OA, CA, and changes to the OA and CA.

(c) Remove DoD programs from special access controls.

(d) Approve the apportionment and deapportionment of DoD SAPs into and out of the IJSTO.

(e) Alter the scope, category, or type of a SAP.

(f) Approve the use of DoD resources to support DoD and non-DoD SAPs, except for those approved under the provisions of Reference (g).

(g) Review foreign access and participation in DoD SAPs.

(2) Provides the SAPOC and Deputy's Management Action Group with recommendations regarding the utility, programmatic, and budgetary considerations of DoD SAPs in support of DoD capability needs and the requirement for an integrated joint force.

(3) Provides recommendations to the DepSecDef and SAPOC regarding SAP management, administration, and oversight for programs submitted for SRG review.

(4) Reviews all waived DoD SAPs annually. Provides recommendations to the SAPOC concerning continued waived status.

(5) Ensures the accuracy of the SAP list submitted to Congress prior to submission of the SAP annual report.

4. SSWG. The SSWG serves as the senior program protection forum to coordinate, deconflict, and integrate special programs; address SAP policy, oversight, and management; and provide recommendations to the SRG.

a. Membership. Members of the SSWG are:

(1) The Director, DoD SAPCO, who serves as the Chair.

(2) The SAPCO Directors of the USD(I), USD(P), USD(AT&L), Army, Air Force, Navy, Marine Corps, JS, Defense Advanced Research Projects Agency, and Missile Defense Agency.

(3) The principal-appointed representatives from the offices of the DCAPE; the DoD CIO; the USD(C)/CFO; and the GC, DoD.

(4) The SSWG Chair may approve additional attendance of appropriately cleared personnel.

b. Primary Functions. The SSWG:

(1) Approves DoD SAPs or DoD SAP sub-elements for inclusion in SAP studies and portfolios, and approve associated billet structures for studies and portfolios, exclusive of Service-initiated study efforts internal to the Military Departments.

(2) Reviews and provides recommendations to the SRG on:

(a) Proposals to establish or disestablish DoD SAPs.

(b) Designation of the OA, CA, and changes to the OA and CA.

(c) Removal of DoD programs from special access controls.

(d) Apportionment and deapportionment of DoD SAPs into and out of IJSTO.

(e) Alteration of the scope, category, or type of a DoD SAP.

(f) Use of DoD resources to support non-DoD SAPs, except for those previously approved under Reference (g).

(3) Conducts an annual revalidation of all DoD SAPs and provides recommendations to the SRG.

(4) Shares information to ensure horizontal protection and standardization, and to capture best practices across all the DoD Components for all DoD SAPs.

(5) Reviews emerging technologies for potential special access protection.

(6) Establishes and tasks the SAP Governance Working Group to develop and recommend SAP policy changes, conduct SAP classification reviews, prepare SAP policy newsletters for approval by the SSWG, and perform other governance duties as assigned.

ENCLOSURE 4

SAP ACCESS PREREQUISITES

1. SAP ACCESS PREREQUISITES. To meet Reference (d) requirements for enhanced security, DoD Components will consider suitability and loyalty criteria to further control SAP access. The sensitivity of the information and the individual's material contribution to the program dictate additional safeguards as approved by the SecDef or DepSecDef. To be accessed to a DoD SAP, the candidate must:

a. Be formally nominated for access by a currently accessed person who can make a NTK and material contribution recommendation to the AAA.

b. Have either a SECRET or TOP SECRET clearance based upon established investigative standards for access to SECRET and TOP SECRET information. The clearance must be based on an appropriate investigation completed within the last 5 years.

c. Have had within the past 12 months a favorable clearance adjudication meeting SCI/SAP eligibility standards without condition, deviation, or waiver, or had a satisfactory review based on the current Standard Form (SF) 86, "Questionnaire for National Security Positions" submitted for most recent personal security investigation. If the SF-86 was submitted for SAP eligibility determination more than 12 months ago, it can either be updated using the original form or a current SF 86C, "Standard Form 86 Certification."

d. Be subject to a random CI-scope polygraph examination. The use of a polygraph examination as a mandatory access determination requirement must be approved by the DepSecDef and consistently applied to all candidates in accordance with DoDI 5210.91 (Reference (o)). 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 DepSecDef. Specific polygraph examinations to resolve issues related to SAP access eligibility will be administered in accordance with Reference (o). CI polygraph examinations are considered current when administered within the past 5 years.

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

2. SAP ACCESS PREREQUISITES FOR FOREIGN NATIONALS. The SecDef and DepSecDef and Director, DoD SAPCO, as delegated in Reference (b), approve SAP access for foreign nationals. The SecDef and DepSecDef may make a specific delegation of this authority to another official in writing. Foreign nationals must maintain an equivalent level of clearance and access to classified information based upon commensurate U.S. standards identified in section 1 of this enclosure and SAP access agreements negotiated with the foreign government.

3. RECIPROCAL ACCEPTANCE OF SAP ACCESS ELIGIBILITY DETERMINATIONS (RECIPROCITY). SAP access eligibility determinations from other DoD Components will be reciprocally accepted unless one or more of the following conditions exist:

a. The nominee's current SAP access is based on an access eligibility waiver approved by another AAA.

b. Substantial information is identified that has not been previously reviewed. (DoD Component SAPCOs are allowed to review the case prior to granting access).

c. The individual does not satisfy a polygraph requirement imposed by the new program.

d. The individual does not satisfy a requirement imposed by the new program that prohibits any non-U.S. immediate family or non-U.S. cohabitant.

e. The personnel security investigation (PSI) upon which an individual has been granted either a SECRET or TOP SECRET clearance is greater than 5 years old.

f. Security clearance does not meet the required level for the SAP.

g. Authenticity of the current or previous SAP access eligibility determination (e.g., authentic AAA; dates in scope) cannot be confirmed.

h. The nominee is a dual citizen of the United States and another country.

4. DETAILED SAP ACCESS ELIGIBILITY PROCEDURES. DoD Components must ensure their SAP access eligibility procedures and standards meet the requirements in this instruction and comply with the guidance contained in E.O. 12968 (Reference (p)) and OMB Policy Memorandum (Reference (q)). DoD-wide SAP access eligibility procedures and standards will be disseminated in a future volume of the DoD SAP Manual no later than 180 days after the publication of this instruction.

ENCLOSURE 5

SAP HIERARCHY

1. HIERARCHY. All SAP and PSAP requests must include proposed hierarchy structures. CA SAPCOs for DoD SAPs, upon adding or deleting compartments, sub-compartments, or projects, must provide current hierarchy structures to the Director, DoD SAPCO. SAP hierarchy structures must include the inheritance policy for each SAP and its subordinate elements. The inheritance structure will be depicted as outlined in Figure 1 and be included in the program hierarchical structures submitted to the Director, DoD SAPCO.

a. The highest element in any SAP hierarchy will be referred to as the "Special Access Program," as defined in the Glossary. This element may also be referred to as an "umbrella" if the SAP has subordinate elements, referred to as compartments, sub-compartments, or projects. Access to the umbrella will include inherited access to all subordinate elements (compartments, sub-compartments, and projects) unless an exception is specifically approved by the CA SAPCO. The SAP and its subordinate elements will be reported to the Director, DoD SAPCO as they are established or disestablished.

b. The hierarchical element immediately subordinate to the SAP will be known as a "SAP compartment," as defined in the Glossary. Compartment(s) will be approved by the CA SAPCO. Access to a compartment will include inherited access to all subordinate elements (sub-compartments and projects) unless an exception is specifically approved by the CA SAPCO. Each compartment and its subordinate elements will be reported to the Director, DoD SAPCO as they are established, inactivated, terminated, or disestablished.

c. A SAP compartment may be established for the sole purpose of identifying the existence of a SAP and administrative information related to that SAP. Such a compartment may stand alone and provide no additional inherited access.

d. The hierarchical element immediately subordinate to the SAP compartment will be known as a "SAP sub-compartment," as defined in the Glossary. Sub-compartment(s) must be approved by the CA SAPCO. Access to a sub-compartment will include inherited access to all subordinate elements unless an exception is specifically approved by the CA SAPCO. Each sub-compartment and its subordinate elements will be reported to the Director, DoD SAPCO as they are established, inactivated, terminated, or disestablished.

e. The hierarchical element subordinate to the sub-compartment will be known as a "SAP project," as defined in the Glossary. Project(s) will be approved by the CA SAPCO and reported to the Director, DoD SAPCO as they are established, inactivated, terminated, or disestablished.

f. Requests for exceptions to the hierarchy structure described in this enclosure will be approved by the CA SAPCO and reported to the Director, DoD SAPCO.

2. TYPE. Upon establishment, DoD SAPS will be identified as acknowledged or unacknowledged. Subordinate elements will be presumed to be within the same type unless otherwise approved by the CA SAPCO and reported as part of the hierarchy structure to the DoD SAPCO. Unacknowledged waived sub-elements added under a non-waived umbrella must be justified, coordinated with the DoD SAPCO, and approved by the DepSecDef.

3. ACCESS MANAGEMENT PLANNING. Some accesses include multiple DoD programs and are used to brief key department personnel whose positions require a wide range of access. For example, the DepSecDef approves access for positions where the incumbents are accessed to all DoD SAPs. Detailed policy related to inclusive access is contained in classified documentation approved by the DepSecDef and retained by the Director, DoD SAPCO.

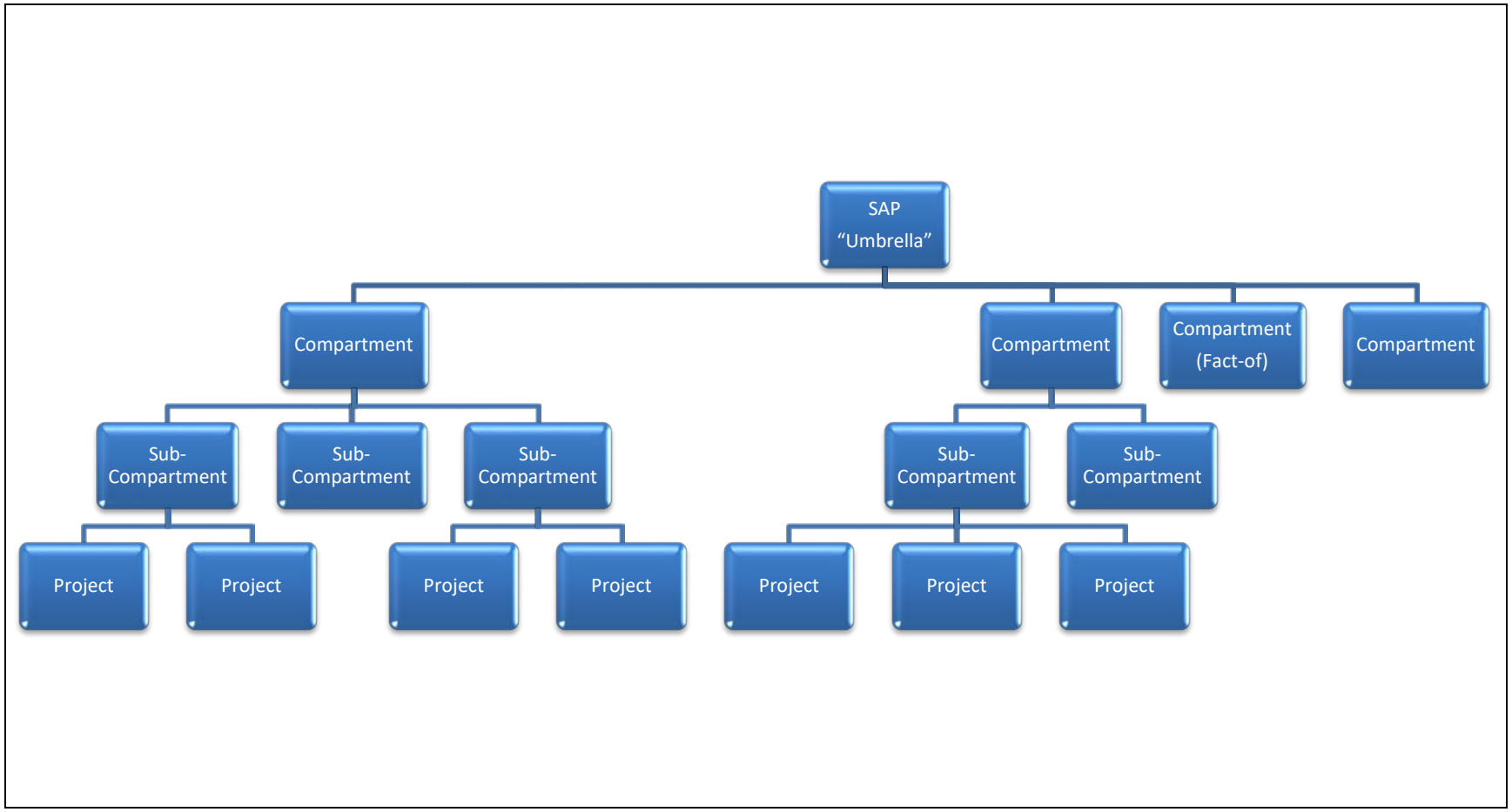
a. An individual with inclusive access may be granted specific program information based on NTK.

b. Designations that provide access to a significant category of programs prefaced by "All" such as "All Acquisition" are made by the Director, DoD SAPCO, and reviewed annually by the SRG for continuation, modification, or termination.

c. DoD SAPs may be designated for inclusion in studies or portfolios when an establishing document, referred to as a Terms of Reference (TOR), has been created that specifically identifies study groups or other groups of people who have a common mission and need to understand SAP capabilities that may impact their specific mission area and which follow an approved billet plan. Study and portfolio groups are initially reviewed and approved by the SSWG. Information provided may be limited to very specific technical information and will only include program inheritance if specifically identified in the TOR.

4. CLASSIFICATION GUIDANCE. Each SAP must have a Security Classification Guide (SCG) signed by an original classification authority completed in accordance with Volume 1 of Reference (c). Classification guidance for compartments, sub-compartments, or projects must be provided either by a separate SCG or based upon written guidance derived from an existing SCG of its umbrella, compartment, or sub-compartment.

Figure 1. Sample Hierarchy



ENCLOSURE 6

SAP LIFE-CYCLE MANAGEMENT

1. SAP ESTABLISHMENT PROCESS

a. The DepSecDef delegates the authority for establishment of PSAPs only to the SAPCO Directors identified in paragraph 4.e above the signature of this instruction. Upon PSAP approval, enhanced security measures may be applied for a period not to exceed 210 days. During this period, funds may only be expended for administrative security reasons. However, if preexisting capabilities or activities are determined to require SAP protection, existing funds appropriated for that purpose may be expended to continue the program. The establishing SAPCO must notify the Director, DoD SAPCO, in writing of the decision to create a PSAP. This decision begins the PSAP timeline as described in Appendix 1 of this enclosure. The notification memo must include:

(1) A program description and structure to include overall scope and proposed compartment, sub-compartment, and project hierarchy.

(2) A program justification for enhanced security measures.

(3) The PSAP type (acknowledged, unacknowledged).

(4) The proposed category (acquisition, operations and support, intelligence).

(5) The proposed CA and OA.

(6) The deconflicted nickname and codeword, as applicable.

(7) The deconflicted PIDs.

(8) The highest level of classification of program material.

(9) A quad chart for the program.

b. The Director, DoD SAPCO, reviews each PSAP submission for accuracy and completeness.

c. The Director, DoD SAPCO, will convene the SSWG to review the PSAP submission for deconfliction.

d. After SSWG review, the Director, DoD SAPCO, must send a letter acknowledging the establishment of the PSAP to the establishing SAPCO.

e. Upon receipt of the letter of acknowledgment, and in accordance with the timeline in Figure 2, the CA SAPCO will commence development of the PSAP package items identified in Figure 3 (see Appendixes 1 and 2 to this enclosure).

f. If the DoD SAPCO recommends against the establishment, the establishing SAPCO may:

(1) Withdraw the PSAP request.

(2) Resubmit a modified PSAP package.

(3) Request review by the SRG as submitted.

g. After notification from the Director, DoD SAPCO, the CA SAPCO will develop the SAP approval package delineated in Figures 3 and 4 for submission to the SRG for formal recommendation.

h. The SRG will review the package and make a formal recommendation for establishment to the SAPOC. When SRG members unanimously agree, the package may be forwarded to the DepSecDef for decision.

i. The SAPOC will review the package and concur or nonconcur in the establishment of the SAP. The SAP establishment package with their comments and recommendations is submitted to the DepSecDef for decision. If approved, the DepSecDef will submit formal notification letters to Congress that the SAP has been established.

j. The SAP may not be initiated until the congressional defense committees are notified of the program and a period of 30 days has elapsed after such notification is received. The Director, DoD SAPCO, must provide a copy of the DepSecDef approval memorandum and the congressional notification letters to the establishing SAPCO.

2. SAP MANAGEMENT AND ADMINISTRATION

a. CA SAPCOs must notify the Director, DoD SAPCO, in writing, of proposals for:

(1) Change of category (acquisition, intelligence, and operations and support).

(2) Change of type (acknowledged, unacknowledged).

(3) Alteration of scope.

(4) IJSTO apportionment or deapportionment.

(5) Disestablishment.

(a) Termination.

(b) Cancellation.

(c) Transition.

(6) Support of non-DoD SAPs.

(7) Addition, deletion, or changes of compartments, sub-compartments, and projects.

(8) Proposals to relieve DSS of NISP security oversight responsibilities (carve-out) when required.

(9) Change of nickname, codeword, PID.

(10) Foreign involvement.

b. CA SAPCO may establish compartments, sub-compartments, and projects when they are consistent with the scope of the DepSecDef approved SAP.

c. Requirements for change of scope to an approved SAP must be recoordinated through the DoD SAPCO to the DepSecDef for decision. The DoD SAPCO must forward documentation for changes to the DepSecDef for approval and legislative notification.

d. Upon notification, the Director, DoD SAPCO, must notify the SSWG membership of the proposed changes. The Director, DoD SAPCO, must also schedule any necessary reviews with the SSWG, SRG, and SAPOC. Following DepSecDef decision, if required, the Director, DoD SAPCO, will provide a copy of the DepSecDef approval or disapproval memo to the CA SAPCO.

e. Whenever a change in the classification of a SAP is planned to be made or whenever classified information concerning a SAP is to be declassified and made public, the DoD SAPCO will provide the congressional defense committees a report containing a description of the proposed change(s), the reasons for change(s), and notice of any public announcement planned to be made with respect to the proposed change(s). This notification is required by Reference (g).

f. The DoD Component heads and the PSAs with CA for DoD SAPs will submit inputs for the SAP annual report to Congress through the Director, DoD SAPCO, for the DepSecDef. The Director, DoD SAPCO, will provide specific guidance to submitting offices via memorandum each year.

g. The DepSecDef approved annual reports will be forwarded to the congressional defense committees by the DoD SAPCO as follows:

(1) SAP Listing. February 1.

(2) SAP Annual Report. March 1.

3. SAP APPORTIONMENT

a. DoD Component and PSA SAPCOs nominate SAP capabilities to be apportioned into IJSTO when they are deemed operationally relevant. SAP capabilities will be nominated for apportionment after they have demonstrated operational capability or no later than (NLT) 18 months prior to plan IOC. When submitting a SAP capability for apportionment to the JS J-3, the DoD Components must provide:

(1) A program quad chart.

(2) A program fact sheet.

(3) An indoctrination briefing.

(4) An SCG.

(5) A written legal review by Component legal counsel.

(6) The PID and nickname. If the entire program is not being transitioned, CA SAPCO must establish a separate compartment, PID, and nickname.

b. The documents submitted must include sufficient information to facilitate Combatant Command planning efforts and contribute to an approved concept of operations.

c. The JS J-3 must process the apportionment request through the SAP governance structure for DepSecDef approval.

4. SAP DISESTABLISHMENT

a. Disestablishment Plan. A program disestablishment plan must be developed when a DoD Component head or PSA with CA elects to terminate, cancel, or transition a SAP. The CA SAPCO must approve the disestablishment plan. The disestablishment plan must address:

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

(2) Administrative actions, which include contracting, fiscal, audit, property disposition, classified material disposition, training, public affairs, legal, logistics, and technical actions. CA SAPCOs must provide the termination plan to the DoD SAPCO. The DoD SAPCO must provide the disestablishment plan to the SSWG for review and determination of any potential impact on other programs.

b. Disestablishment Approval. The DoD SAPCO must prepare the action memo for DepSecDef approval and prepare DepSecDef congressional notification letters for signature and notification to Congress.

5. PROGRAM PROTECTION PLANS (PPPs). Reference (l) requires the development of PPPs, to include critical program information (CPI), in accordance with DoDI 5200.39 (Reference (r)). DoD SAP program managers must develop PPPs or an alternative document that combines program protection and other aspects of program security.

Appendixes

1. PSAP Checklist Timeline
2. SAP Approval Package Checklist
3. Sample Action Memo With Sample Markings

APPENDIX 1 TO ENCLOSURE 6

PSAP CHECKLIST TIMELINE

Figure 2. PSAP Checklist Timeline

P[1] – CA signs PSAP establishment memo and provides memo to DoD SAPCO NLT[2] P+7 – DoD SAPCO provides acknowledgement memo to CA SAPCO - Deconflicts nickname, codeword, and PID consistent with Reference (e) - Enters PIDs, codewords, and nicknames into appropriate database - Schedules SSWG - Distributes CA letter and DoD SAPCO acknowledgement memo to SSWG membership NLT P+14 – SSWG reviews PSAP - Programmatic deconfliction - Validation - Written recommendation NLT P+45 – CA submits draft SCG to DoD SAPCO NLT P+60 – DoD SAPCO provides comments on SCG NLT P+90 - CA submits SAP approval package (see Table 3) to DoD SAPCO for distribution to SRG members NLT P+105 – SRG convenes and comments on SAP approval package NLT P+130 – Final SAP approval package to DoD SAPCO for distribution to SAPOC NLT P+150 – Convene SAPOC for recommendation to DepSecDef NLT P+180 – DepSecDef decision. Congressional notification or PSAP termination as appropriate NLT P+210 – End of 30-day period without Congressional decision
1. P = Date of PSAP establishment 2. NLT = no later than

APPENDIX 2 TO ENCLOSURE 6

SAP APPROVAL PACKAGE CHECKLIST

Figure 3. SAP Approval Checklist

1. Quad Chart

2. Type, Category, and Classification of SAP. If unacknowledged and reporting requirements are to be waived, attach justification to waive the requirements of Volumes 2A and 2B of DoD 7000.14-R (Reference (s)).

3. CA

4. OA

5. Relationships. Identify relationship(s), if any, to other SAPs. Include existing agreements, MOUs, and similar SAP arrangements, to include NATO-related programs under various NTK regimes.

6. Legal Review. A written legal review by Component legal counsel conducted to ensure program complies with law (domestic and international).

7. Program Budgetary Information (or stipulate no funding and/or content only)

8. Access Limits. The SAP access limit for the first year is _____. Estimate the numbers falling in each category below:

   a. Component: _____

   b. Other DoD: _____

   c. Contractors: _____

   d. Other (private sector): _____

9. Polygraph Requirement. As a condition of access if applicable.

10. Security Classification Guide.

11. Program Security Policy and Procedures Plan. Addressing:

   a. Program protection.

   b. An arms control plan that addresses treaty considerations.

   c. A disclosure plan that complies with Reference (j) if any release of SAP information to another nation or foreign nationals is anticipated.

   d. Contract strategy (carve-out justification if applicable).

   e. Archive of program information.

   f. Threat or vulnerability assessment.

   g. Applicable Operations Security (OPSEC) measures in accordance with DoDD 5205.02E (Reference (t)).

APPENDIX 3 TO ENCLOSURE 6

SAMPLE ACTION MEMO WITH SAMPLE MARKINGS

Figure 4. Sample Action Memo Recommending SAP Establishment

THIS SAMPLE IS UNCLASSIFIED

[PLACE APPROPRIATE SECURITY CAVEATS IN HEADER]
[USE TIMES NEW ROMAN 12 POINT FONT.]

ACTION MEMO

[Month Day, Year, Time]

FOR: DEPUTY SECRETARY OF DEFENSE

FROM: Name [and military rank and Service if appropriate], Director, DoD Special Access Program Central Office

SUBJECT: (S//SAR-GTE) Establishment of Special Access Program (SAP) GREEN TREE

(S//SAR-GTE) I am requesting that you approve the establishment of GREEN TREE (GTE) as a DoD unacknowledged operations and support SAP that protects the collection and exploitation of various types of foreign military critical car parts.

(S//SAR-GTE) Current planned unacknowledged sub-compartments of GTE are LEAF BARK (LBK), which protects reports generated during exploitation efforts, and COTTON WATER (CWR), which protects relationships with foreign partners related to acquisition of car parts.

(U//HVSACO) The GTE cognizant authority is [enter appropriate information] and the Army, and the oversight authority is the Under Secretary of Defense for Personnel and Readiness.

(U) The Army will be the cognizant security agency. The Defense Security Service will be carved out from its normal industrial security oversight responsibilities.

(U//HVSACO) Access to GTE will require completion of a Counterintelligence (CI)-Scope polygraph examination administered upon initial access and periodically thereafter at no more than 5 year intervals.

(U) The [Senior Review Group/SAPOC] briefing at TAB A provides additional information. The program quad chart is attached at TAB B. Congressional notification letters of the establishment of this SAP, consistent with 10 U.S.C Sec. 119(f) are at TAB C.

(S//SAR-GTE) RECOMMENDATION: That you approve GTE as an unacknowledged SAP and authorize carve-out status and the mandatory administration of CI polygraphs, and that you sign the notification letters to Congress (TAB C) identifying GREEN TREE as a new SAP.

Approve: _____ Disapprove: _____ Date: _____

COORDINATION: TAB D

[PLACE APPROPRIATE SECURITY CAVEATS IN FOOTER]

ENCLOSURE 7

PROGRAM RECORD FILES

1. PROGRAM RECORD FILES. The DoD Component and PSA SAPCOs with CA will maintain record files for each of their DoD SAPs, compartments, sub-compartments, and projects. At a minimum, each SAP record file must include:

a. Documentation approving the SAP:

(1) Written approval by SecDef or DepSecDef of carve-out status when DSS is relieved of industrial security oversight responsibilities.

(2) The identification of SAP facilities (or identification of the SAPCO-approved database that contains the information) that have been carved-out based upon this authority.

(3) Initial written legal review by Component legal counsel.

b. Designations of program access approval authorities, program managers, and program directors, and of program security officials.

c. A copy of each SAP annual report to Congress, including the revalidation statement that continued SAP status is warranted.

d. The Program Objective Memorandum and the President's Budget Decision Review of issue papers.

e. Budget exhibits as required by Reference (q).

f. Legislative history of the SAP.

g. Identification and location of prime contractor(s) and subcontractor(s) performing classified work (or identification of the SAPCO approved database that contains the information) under the SAP.

h. SAP access rosters or an electronic database, both current and historical (or identification of the SAPCO approved database that contains the information), program indoctrination agreements, and records of inadvertent disclosure.

i. Foreign disclosure case files.

j. Current and historical SCGs, security procedures guides, or program security plans, as applicable. These may be hard copy or electronic copy. Electronic copies must be provided to the DoD SAPCO for all SAP SCGs created after the publication date of this instruction.

k. Documented staff assistance visits and security inspection reports for program locations, or the location of the report if stored centrally or electronically.

l. Reports related to, but not limited to, legal, fiscal, audit, investigative, operational, statutory, or regulatory oversight functions if authorized.

m. Correspondence addressing:

(1) Proposal to establish or terminate DoD SAP.

(2) Designation of and change to the OA and CA.

(3) Removal of DoD program from special access control.

(4) Apportionment and deapportionment of DoD SAP into and out of IJSTO.

(5) Alteration of the scope, category, or type of a DoD SAP.

(6) Use of DoD resources to support non-DoD SAP.

(7) Written legal reviews by Component legal counsel.

2. RETENTION OF PROGRAM DATA. Within 6 months of being approved as a SAP, CA SAPCO will coordinate with the DoD Component records management programs to develop long-term retention of program data, to include archiving of information and hardware of historical value in accordance with DoDI 5015.02 (Reference (u)).

ENCLOSURE 8

JS AND COMBATANT COMMAND SAP PROCEDURES

1. GENERAL. Any granting of SAP access to JS and Combatant Command personnel must be coordinated with the JS SAPCO. Additionally, any granting of access to Combatant Command personnel and personnel assigned to sub-unified commands, joint functional component commands (JFCCs) or joint task forces (JTFs), must also be coordinated with the appropriate Combatant Command SAP Control (SAPCON) Office and the JS SAPCO. Access of Service component personnel must be in accordance with Service procedures. When the Combatant Command SAPCON Office accesses Service component personnel, they assume responsibility for annual reviews and SAP refresher training.

2. JS SAP PROCEDURES. The JS SAPCO serves as the only entry point for any DoD SAPs into the JS. Any organization or program office, to include non-DoD agencies, desiring to access JS personnel to a program must contact the JS SAPCO before taking any action. The JS SAPCO:

a. Ensures all eligibility reviews (initial and annual) and annual SAP refresher training for the JS personnel is completed by appropriately trained and designated personnel.

b. Accredits all SAP facilities and information systems (ISs) for the JS and Combatant Commands unless delegated to the Combatant Command SAP Control Officer or SAP Security Manager (SAPSM).

c. Approves all SAP MOAs, MOUs, and co-utilization agreements (CUAs) for the JS.

3. COMBATANT COMMAND SAP PROCEDURES

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

b. Each Combatant Command has designated a Combatant Command SAPSM who serves as the central coordination official for the command for SAP personnel, physical, information, and IT security. The SAPSM:

(1) Ensures all eligibility reviews (initial and annual) and annual SAP refresher training for assigned personnel are completed by appropriately trained and designated personnel.

(2) Ensures annual SAP refresher training is conducted for individuals assigned to the Combatant Command, Sub-Unified commands, JFCCs, JTFs, and any Service component personnel accessed through the Combatant Command SAPCON office.

(3) Coordinates the accreditation of SAP facilities and ISs for the Combatant Command.

(4) Drafts all SAP MOAs, MOUs, and CUAs for Combatant Command SAPCON Officer approval and coordination with JS SAPCO.

c. Annually, the JS SAPCO, in coordination with the CA SAPCOs, develops Combatant Command SAP core portfolios for DoD SAPCO approval. Each portfolio is uniquely based upon the Command's mission, area of operations, and threat. The Combatant Commands maintain DoD SAPCO-approved billet structures for their core portfolio of DoD SAPs.

d. Combatant Commands may also request the creation of additional SAP billet structures, called functional billet groups (FBGs) that allow for additional access to programs from the core portfolio for Combatant Command action officers necessary to execute specific non-apportioned SAP-related functional tasks on a recurring basis. The JS SAPCO, in coordination with the CA SAPCOs:

(1) Establishes the FBGs and submits them for DoD SAPCO approval.

(2) Reviews the FBGs annually for continued relevance to command mission and recommends modification or termination.

4. U.S. SPECIAL OPERATIONS COMMAND (USSOCOM) UNIQUE PROCEDURES. USSOCOM will maintain a SAPCO that exercises the authorities listed in section 5 of Enclosure 2 of this instruction. The procedures listed in sections 1 through 2 of this enclosure only apply to those DoD SAPs for which USSOCOM is not the CA.

ENCLOSURE 9

FOREIGN DISCLOSURE PROCEDURES

1. GENERAL. All disclosure of classified military information must be in accordance with U.S. national and DoD policy pursuant to National Disclosure Policy (NDP)-1 (Reference (v)). Classified military information will be released only within the constraints authorized by officials designated consistent with Reference (v).

a. The disclosure authorization process details the specific information, equipment, capabilities to be released, and those items that are not to be released. All disclosures of classified military information and its associated unclassified technical information must be approved for foreign release.

b. In parallel with the disclosure process is security vetting for access to SAP information. The SAP access approval process addresses who is eligible to receive the SAP information; the disclosure process determines what specific information those deemed eligible may receive, and in what form they may receive it. The two authorizations are mutually supporting in guiding the release of SAP information, equipment, and capabilities.

2. PROCEDURES OVERVIEW. There are two basic elements in the disclosure process. First is obtaining approval at the appropriate level of authority to release the information. The second is creation and approval by a designated disclosure authority of a Delegation of Disclosure Authority Letter (DDL), which provides guidance on the scope and limitations of information to be released.

a. Release Approval. The SecDef or DepSecDef must approve all instances of foreign release of SAP information, equipment, and capabilities unless such release has been previously delegated in writing to another senior official or component head. Requests to authorize the disclosure of SAP information will be routed through the Director, DoD SAPCO, to the DepSecDef.

b. DDL. The DDL provides the details of the release authorization. It includes highest classification and caveats approved for release, identifies approved disclosure methods (oral, visual, or documentary), clearly identifies categories of information permitted (see Reference (v)), the scope of the release (who may release and to whom), specific information authorized for release, specific information prohibited from release, special release and security procedures, and any authority to delegate authority to subordinate activities. The DDL will be approved by a designated disclosure authority whose officially designated authority extends to the SAP information being authorized for disclosure. The DDL will be structured according to the guidance provided in Reference (v), and must be followed by all persons authorized to provide foreign disclosure of the information. Categories of information that may be designated in a DDL are found in Reference (v).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AAA	access approval authority
ACCM	alternate compensatory control measures
CA	cognizant authority
CFIUS	Committee on Foreign Investment in the United States
CI	counterintelligence
CIO	Chief Information Officer
CPI	critical program information
CSA	cognizant security authority
CUA	co-utilization agreement
DCAPE	Director, Cost Assessment and Program Evaluation
DCIO	Defense Criminal Investigative Organization
DDL	Delegation of Disclosure Authority Letter
DepSecDef	Deputy Secretary of Defense
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
DSS	Defense Security Service
E.O.	Executive order
EXCOM	Executive Committee
FBG	functional billet group
GC, DoD	General Counsel of the Department of Defense
HVSACO	Handle Via Special Access Controls Only
IJSTO	Integrated Joint Special Technical Operations
IOC	initial operational capability
IT	information technology
JFCC	Joint Functional Component Command
JS	Joint Staff
JTF	joint task force
LO/CLO	low observables/counter low observables
MOA	memorandum of agreement
MOU	memorandum of understanding

NDP	National Disclosure Policy
NID	national interest determination
NISP	National Industrial Security Program
NLT	no later than
NTK	need to know
OA	oversight authority
PID	program identifier
PPP	program protection plan
PSA	principal staff assistant
PSAP	prospective Special Access Program
PSI	personnel security investigation
SAP	Special Access Program
SAPCO	Special Access Program Central Office
SAPCON	Special Access Program control
SAPOC	Special Access Program Oversight Committee
SAPSM	Special Access Program Security Manager
SCG	security classification guide
SecDef	Secretary of Defense
SF	standard form
SRG	Senior Review Group
SSWG	Special Access Program Senior Working Group
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy

PART II. DEFINITIONS

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

access eligibility review. The procedure addressing the suitability indicators of the person recommended for SAP access. It is used during the initial SAP eligibility determination process and is also applied during annual reviews of personnel security questionnaire updates or to address issues identified (self or third-party) that may impact an individual's ability to adequately protect SAP information.

access eligibility waiver. Access eligibility granted or continued despite the presence of substantial issue information that would normally preclude access.

access limits. A pre-established limit on the number of personnel who are accessed to a particular program or compartment. Access limits are approved by the DoD Component SAPCO.

acknowledged SAP. A SAP whose existence is acknowledged, affirmed, or made known to others, but its specific details (technologies, materials, techniques, etc.,) are classified as specified in the applicable SCG.

acquisition SAP. A SAP established to protect sensitive research, development, testing and evaluation, modification, and procurement activities.

apportioned SAP. A SAP that is formally included in the IJSTO process for Combatant Command use during deliberate planning, crisis action response, and operational employment.

billet plan. A formal, pre-approved access listing that is position-based. Provides the NTK for individuals assigned to pre-approved positions (billets).

carve-out. A provision approved by the SecDef or DepSecDef that relieves DSS of its NISP obligation to perform industrial security oversight functions for a DoD SAP.

code word. A single word assigned a classified meaning by appropriate authority to ensure proper security concerning intentions and to safeguard information pertaining to actual, real-world military plans, activities or operations classified CONFIDENTIAL or higher.

content only. A descriptive term used to describe a SAP (or any sub-element) that contains information only and either has no funding associated with it or its funding is managed as part of the DoD unclassified corporate budget process.

CPI. Elements or components of a SAP that, if compromised, could cause significant degradation in mission effectiveness, shorten the expected combat-effective life of the system, reduce technological advantage, significantly alter program direction, or enable an adversary to defeat, counter, copy, or reverse-engineer the technology or capability.

DCIO. DCIOs include the U.S. Army Criminal Investigation Command, Naval Criminal Investigative Service, Air Force Office of Special Investigations, and Defense Criminal Investigative Service. DCIOs conduct criminal investigation related to DoD SAPs when need-to-know has been established and access granted.

HVSACO. 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, approved SAP communications systems, SAP facilities, or SAP-approved storage areas.

intelligence SAP. SAP established primarily to protect planning and execution of especially sensitive intelligence or CI operations or collection activities.

level of access. Identifies the clearance (TOP SECRET or SECRET) required for access to a SAP or included compartment, sub-compartment, or project.

MOA. Written agreement among relevant parties that specifies roles, responsibilities, terms, and conditions for each party to reach a common goal. MOAs are required when SAP resources are committed between programs, components of the DoD, or non-DoD components.

MOU. Written agreements between programs that do not obligate SAP resources. MOUs will be executed when it is necessary to exchange SAP information between Services.

nickname. A combination of two separate unclassified words that is assigned an unclassified meaning and is employed only for unclassified administrative, morale, or public information purposes.

operations and support SAP. SAP established to protect the planning for, execution of, and support to especially sensitive military operations.

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

program identifier (PID). An unclassified three-letter acronym or abbreviated identifier for an assigned SAP nickname or codeword. PID letters will be drawn from the letters within the nickname or codeword.

program disestablishment. The action taken when active enhanced security protective measures are no longer required for the information contained within the program.

program termination. A SAP, compartment, sub-compartment, or project whose activities have ceased and will not be restarted. SAP security measures are still required.

program transition. An action that results in a change in protection level for the SAP material such as SAP to non-SAP, classified to unclassified, or the transfer of information to another SAP or compartment.

PSAP. A DoD program or activity for which enhanced security measures have been proposed and approved to facilitate security protections prior to establishing the effort as a SAP.

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.

SAP. A program activity which has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by an SCG.

SAP compartment. An effort under a SAP, approved by the CA SAPCO and protected by a separate SCG or based upon written guidance derived from the existing SCG of its umbrella. A person accessed to a compartment is also accessed to all subordinant elements (sub-compartments and projects), unless an exception is specifically approved by the CA SAPCO.

SAP project. A narrowly-focused, short-term effort under a SAP sub-compartment approved by the CA SAPCO, or designee that is protected by a specific SCG or based upon written guidance derived from an existing SCG of its parent compartment or sub-compartment. Projects may be identified by nicknames, codewords, or alpha-numeric characters.

SAP sub-compartment. An effort under a SAP compartment approved by the CA SAPCO and protected by a distinct and separate SCG or based up written guidance derived from an existing SCG of its SAP compartment. A person accessed to a sub-compartment is also accessed to all subordinant elements (additionl sub-compartments and projects), unless an exception is specifically approved by the CA SAPCO.

SCG. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

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

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 SecDef has waived applicable reporting in accordance with Reference (c) following a determination of adverse effect to national security. 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.