



Department of Defense DIRECTIVE

NUMBER 5205.07

January 5, 2006

Incorporating Change 1, February 25, 2008

USD(I)

SUBJECT: Special Access Program (SAP) Policy

- References:
- (a) DoD Directive O-5205.7, subject as above, January 13, 1997
(hereby canceled)
 - (b) *Deputy Secretary of Defense Memorandum, "Change to the Special Access Program Oversight Committee Membership," December 3, 2007*
(hereby canceled)
 - ~~(bc)~~ Section 119 of title 10, United States Code
 - ~~(ed)~~ DoD Instruction O-5205.11, "Management, Administration, and Oversight of DoD Special Access Programs (SAPs)," July 1, 1997
 - ~~(de)~~ through ~~(jk)~~, see Enclosure 1

1. REISSUANCE AND PURPOSE

This Directive:

1.1. Reissues reference (a) to update policy and responsibilities on the oversight and management of all DoD Special Access Programs (SAPs). *Incorporates and cancels Reference (b).*

1.2. Re-establishes and updates the responsibilities and functions of the DoD SAP Oversight Committee (SAPOC) and its supporting structure, including the Senior Review Group (SRG) and the DoD SAP Central Office (DoD SAPCO).

2. APPLICABILITY AND SCOPE

2.1. This Directive applies to:

2.1.1. The Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, 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 Department of Defense (hereafter referred to collectively as the “DoD Components”).

2.1.2. Contractors and consultants of the DoD Components when contract performance depends on access to DoD SAPs.

2.1.3. Non-DoD U.S. Government Agencies whose personnel, by mutual agreement, require access to DoD SAPs.

2.1.4. All DoD SAPs and any non-DoD SAPs for which the Deputy Secretary of Defense has approved the use of DoD resources (e.g., personnel and funding).

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 2.

4. POLICY

It is DoD policy that:

4.1. Only the Secretary or the Deputy Secretary of Defense shall:

4.1.1. Render the final decision on proposals to establish or terminate DoD SAPs, alter the scope of DoD SAPs, and use DoD resources to support non-DoD SAPs.

4.1.2. Establish and resource the DoD SAPCO, and appoint a Director, DoD SAPCO. The DoD SAPCO shall be the primary point of contact with Agencies of the Executive Branch, Congress, and the DoD Components on all issues relating to DoD SAPs.

4.2. DoD SAPs shall be established and maintained when absolutely necessary to protect the Nation’s most sensitive information or when required by statute. Establishment shall be consistent with Section 119 of title 10, United States Code (reference ~~(b)(c)~~), approved by the Deputy Secretary of Defense, and based on a determination that the threat and/or vulnerability warrants protection that exceeds that normally required for information at the same classification level.

4.3. The DoD SAPOC shall advise and assist the Secretary and the Deputy Secretary of Defense in the management and oversight of DoD SAPs. The SAPOC shall review all DoD SAPs annually and assess the department’s involvement with and commitment to non-DoD SAPs.

4.3.1. Members of the DoD SAPOC are the Deputy Secretary of Defense (Chair); the Under Secretary of Defense For Acquisition, Technology, and Logistics (USD(AT&L)) (Vice Chair); the Under Secretary of Defense For Policy (USD(P)); the Under Secretary of Defense

(Comptroller)/Chief Financial Officer; the Under Secretary of Defense for Intelligence (USD(I)); *the Vice Chairman of the Joint Chiefs of Staff*; the Assistant Secretary of Defense For Networks and Information Integration (ASD(NII)); *the DoD General Counsel*; the Director, Program Analysis and Evaluation; ~~the DoD General Counsel; the Vice Chairman of the Joint Chiefs of Staff~~; the Under Secretaries of the Army, the Navy, and the Air Force; *the Army and the Air Force Vice Chiefs of Staff; the Vice Chief of Naval Operations; the Assistant Commandant of the Marine Corps*; and the Director, DoD SAPCO (Executive Secretary).

4.3.2. ~~The SRG, comprised of a senior individual to be designated by each permanent member of the SAPOC;~~ *The SRG* is established to perform the principal working-level support functions for the SAPOC. *Each permanent member of the SAPOC designates a senior individual to represent that member on the SRG. However, in the case of the Army, Navy, and Air Force, only one individual will represent both its Under Secretary and Vice Chief.*

4.3.3. DoD Instruction O-5205.11 (reference ~~(e)~~(d)) further amplifies the functions of the DoD SAPOC, the SRG, and other support offices.

4.4. DoD SAPs shall be protected at all times with controls established and maintained to ensure that classified SAP information is used, discussed, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons. DoD SAPs shall conform to all laws and DoD issuances relating to or governing DoD SAPs.

4.5. Personnel security requirements for DoD SAPs shall be according to Executive Order 12968 (reference ~~(d)~~(e)) and access to SAP information shall be based on a final SECRET clearance with a favorable National Agency Check, Local Agency Check(s), and a Credit Check all less than 5 years old, and a favorable tier review. Eligibility shall be considered current if the person has been in continuous access since their last investigation and their request for periodic re-evaluation was submitted within 5 years of their last investigation date. Persons with current eligibility shall not be precluded from access to additional SAPs while their reinvestigations are active. The program cognizant authority may authorize the use of an interim security clearance as a basis for granting access to DoD SAPs in exceptional circumstances.

4.6. Approving officials, or their designee, shall record all favorable and unfavorable SAP access eligibility determinations. All approving officials (including designees) shall be knowledgeable of the DoD adjudication standards for SAP access, due process procedures and reciprocity principles prior to making any access determinations. Only government adjudicators shall issue denials of access eligibility.

4.7. An individual with an existing SAP access, granted without exception, condition or waiver, shall not be denied access to another SAP of the same sensitivity level as long as the individual has a need for access to the information involved.

4.8. All personnel having access to DoD SAPs are subject to a random Counterintelligence (CI)-scope polygraph examination. However, using a polygraph examination as an access determination requirement shall be a condition specifically approved by the Deputy Secretary of

Defense in conjunction with the establishment of the SAP and consistently applied to all candidates according to DoD Directive 5210.48 (reference ~~(e)~~(f)). CI-scope polygraph examinations shall not be used as the only basis for granting access to DoD SAPs.

4.9. According to DoD Directive 5010.38 (reference ~~(f)~~(g)), the DoD Management Control Program (MCP) shall be implemented within all DoD SAPs. To ensure adequate implementation, the DoD Components having SAP cognizant authority are required to have MCP coordinators within special access channels.

4.10. DoD employees assigned legal, fiscal, investigative, operational, or statutory oversight duties for SAPs shall be deemed to have a need-to-know for access and shall be granted effective and sufficient access to those programs to meet their responsibilities.

5. RESPONSIBILITIES

5.1. The Under Secretary of Defense for Intelligence shall:

5.1.1. Serve as the oversight authority for all DoD Intelligence SAPs and those SAPs delegated to the USD(I) for oversight.

5.1.2. Establish an OSD-level SAP Coordination Office and designate a Director for this office. The USD(I) SAP Coordination Office shall support the USD(I) in carrying out his oversight and management responsibilities for SAPs under his authority. Responsibilities of this office include, but are not limited to, processing documents required for approval, annual validation, and Congressional reporting of SAPs, issuing nicknames and code words assigned to OSD program activities according to procedures issued by the Chairman of the Joint Chiefs of Staff, and serving as the SAP Coordination Office for the ASD(NII)/DoD Chief Information Officer.

5.1.3. Develop, coordinate, and promulgate all DoD SAP security policies.

5.1.4. Perform oversight of the DoD Components managing SAP equities to ensure security policies and guidance are implemented.

5.1.5. Oversee and, if necessary, direct credentialed CI personnel to investigate security violations, infractions, or CI matters within DoD SAPs.

5.1.6. Direct the Director, Defense Security Service to maintain a sufficient cadre of SAP-trained personnel to provide periodic security reviews for contracts or similar agreements entered into established to support DoD SAPs. This requirement does not apply to SAPs that employ alternative oversight mechanisms approved by the Secretary or the Deputy Secretary of Defense.

5.1.7. Direct the Directors of the Defense Intelligence Agency, National Security Agency, National Reconnaissance Office and National Geospatial-Intelligence Agency to maintain a sufficient cadre of SAP-trained personnel to perform agency-unique tasks associated with SAPs.

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics shall:

5.2.1. Serve as the oversight authority for those DoD Acquisitions SAPs delegated to the USD(AT&L) for oversight.

5.2.2. Establish an OSD-level SAP Coordination Office and designate a Director for this office. The USD(AT&L) SAP Coordination Office shall support the USD(AT&L) in carrying out his oversight and management responsibilities for SAPs under his authority. Responsibilities of this office include, but are not limited to, processing documents required for the approval, annual validation, and Congressional reporting of SAPs.

5.2.3. Direct the Directors of the Defense Logistics Agency, Missile Defense Agency, Defense Advanced Research Projects Agency, and Defense Contract Management Agency to maintain a sufficient cadre of SAP-trained personnel to perform agency-unique tasks associated with SAPs.

5.3. The Under Secretary of Defense for Policy shall:

5.3.1. Serve as the oversight authority for DoD Operations and Support SAPs delegated to the USD(P) for oversight.

5.3.2. Establish an OSD-level SAP Coordination Office and designate a Director for this office. The USD(P) SAP Coordination Office shall support the USD(P) in carrying out his oversight and management responsibilities for SAPs under his authority. Responsibilities of this office include, but are not limited to, processing documents required for the approval, annual validation, and Congressional reporting of SAPs.

5.3.3. Ensure SAPs are integrated into and consistent with the development of national security and defense strategies, plan development, and contingency operations. Funds shall be programmed to support responsibilities assigned in DoD Directive 5111.1 (reference ~~(g)~~(h)).

5.3.4. Provide oversight and guidance to SAP managers within the Office of the USD(P) and its components.

5.3.5. Establish and operate the OSD Special Technical Operations office to coordinate and process DoD issues with the Integrated Joint Special Technical Operations element, the Office of the Chairman, Joint Chiefs of Staff.

5.3.6. Develop, coordinate, promulgate, and oversee the implementation of Special Security Countermeasures Policy, including those associated with arms control and non-proliferation initiatives that could impact DoD sensitive equities.

5.4. The Director, DoD SAPCO shall:

5.4.1. Serve as the Executive Secretary of the SAPOC.

5.4.2. Develop, coordinate, and publish DoD SAP management policy, instructions, and publications.

5.4.3. Direct and supervise the collection, integration, and analysis of specific program information to support SAPOC deliberations and decisions.

5.4.4. Establish and implement a DoD-wide SAP naming convention to identify SAPs, facilitate recognition and tracking, and prevent confusion.

5.4.5. Serve as the principal point of contact in the Department of Defense for all SAP resources.

5.4.6. Act as the DoD legislative liaison for all DoD SAPs.

5.5. The Under Secretary of Defense (Comptroller)/Chief Financial Officer shall direct the Director, Defense Contract Audit Agency to maintain a sufficient cadre of SAP-trained personnel to provide audit support to DoD SAPs.

5.6. The Director, Program Analysis and Evaluation shall:

5.6.1. Develop and provide Program Objective Memorandum (POM) preparation instructions for SAP POM submissions.

5.6.2. Evaluate SAPs in light of projected threats, estimated costs, resource constraints, and U.S. defense objectives and priorities.

5.6.3. Participate in the budget and program reviews for SAPs.

5.7. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer shall maintain a sufficient cadre of SAP-trained personnel to perform assigned responsibilities for Sensitive Information Integration.

5.8. The Inspector General of the Department of Defense shall maintain a sufficient cadre of SAP-trained personnel to perform inspection, investigative, and audit functions for DoD SAPs and SAP-related activities.

5.9. The Assistant to the Secretary of Defense for Intelligence Oversight shall:

5.9.1. Maintain a sufficient cadre of personnel with clearances and accesses adequate to perform intelligence oversight inspections of DoD intelligence SAPs according to DoD Directive 5148.11 (reference ~~(i)~~).

5.9.2. Ensure that the audit functions required by DoD Directive 5240.12 (reference ~~(j)~~) are performed.

5.9.3. Review the CI support provided to specifically-identified DoD SAPs to verify compliance with reference ~~(j)~~ and DoD Directive 5240.2 (reference ~~(k)~~).

5.10 The Heads of the DoD Components shall:

5.10.1. Establish a Component-level SAPCO to execute, manage, administer, oversee, and maintain records on the SAPs they exert cognizant authority over.

5.10.2. Submit any administrative SAP action requiring SAPOC review or approval to the appropriate OSD-level SAP Coordination Office. This includes, but is not limited to, recommendations on establishment, disestablishment, category, scope, sensitivity level, management procedures, and mission change(s) of DoD SAPs.

5.10.3. Ensure that all relevant SAP information, including SAP accesses, SAP program and budget information, program security information, cover support and treaty requirements data are maintained in a segregated data archive. This data archive shall be current to facilitate the timely submission of accurate information to the DoD SAPCO.

5.10.4. Maintain a sufficient cadre of SAP-trained personnel to perform programmatic, security and administrative tasks associated with SAPs unless specifically exempted.

5.10.5. Ensure current arms control compliance requirements, obligations, and constraints are considered as an integral part of the policy, planning, operations, and acquisition process for the SAPs they exert cognizant authority over.

5.10.6. Use their organic or servicing CI organizations to provide complete CI support to DoD SAPs according to reference ~~(k)~~.

5.10.7. Ensure security violations involving compromise or suspected compromise of SAP information are reported to the Component-level or the OSD-level SAP Coordination Office.

5.10.8. Notify the Director, CI Field Activity, whenever a CI inquiry or investigation is opened on an individual with SAP access.

5.10.9. Submit SAP establishment requests through the appropriate Under Secretary of Defense to the DoD SAPCO for presentation to the SRG and SAPOC. The SAPOC shall provide the Deputy Secretary of Defense with its recommendations for the category of the SAP, its oversight authority, and its cognizant authority.

5.10.10. Maintain a listing of all SAP facilities they manage and provide such information to authorized recipients if requested.

5.11. The Chairman of the Joint Chiefs of Staff shall:

5.11.1. Establish a Component-level SAP Coordination Office that reviews and disseminates planning information concerning the operational aspects of apportioned DoD SAPs and designate a Director for this office.

5.11.2. Manage and operate a joint process to ensure the Combatant Commanders and designated members of their staff are afforded knowledge of current and emerging SAP protected systems, technologies, and methodologies as well as currently available SAP protected weapon systems and end items appropriate to their mission.

6. EFFECTIVE DATE

This Directive is effective immediately.



Gordon England

Enclosures - 2

- E1. References, continued
- E2. Definitions

E1. ENCLOSURE 1

REFERENCES (continued)

- (e) Executive Order 12968, "Access to Classified Information," August 4, 1995
- (ef) DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1984
- (fg) DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996
- (gh) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P)),
December 8, 1999
- (hi) DoD Directive 5148.11, "Assistant to the Secretary of Defense for Intelligence Oversight," May 21, 2004
- (ij) DoD Directive 5240.12, "Department of Defense (DoD) Intelligence Commercial Activities (ICAs)," December 2, 1992
- (jk) DoD Directive 5240.2, "DoD Counterintelligence (CI)," May 22, 1997

E2. ENCLOSURE 2

DEFINITIONS

E2.1. Acknowledged Special Access Program (SAP). An existing SAP whose overall purpose is identified and its specific details, technologies, materials, techniques, etc., of the program are classified as dictated by their vulnerability to exploitation and risk of compromise.

E2.2. Acquisition SAP. A SAP established to protect sensitive research, development, testing and evaluation, modification or procurement activities.

E2.3. Cognizant Authority. The DoD Component or Agency accountable for management and execution of their respective DoD SAPs.

E2.4. DoD SAP. Any DoD program or activity employing enhanced security measures (e.g. safeguarding, access requirements, etc.) exceeding those normally required for collateral information at the same level of classification shall be established, approved, and managed as a DoD SAP.

E2.5. Intelligence SAP. A SAP established primarily to protect the planning and execution of especially sensitive intelligence or CI operations or collection activities.

E2.6. Operations and Support (O&S) SAP. A SAP established primarily to protect the planning for, execution of, and support to especially sensitive military operations. An O&S SAP may protect organizations, property, operational concepts, plans, or activities.

E2.7. Oversight Authority. The Senior DoD Official (e.g., the USD(AT&L), the USD(P), or the USD(I)) assigned primary oversight. Oversight responsibilities include, but are not limited to, endorsing change of category, conducting program reviews, endorsing termination or transition plans, ensuring SAPs do not duplicate or overlap, coordinating and forwarding SAP annual reports to the DoD SAPCO.

E2.8. Unacknowledged SAP. A SAP having protective controls ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.

E2.9. Waived SAP. An unacknowledged SAP for which the Secretary of Defense has waived applicable reporting requirements of reference ~~(b)~~(c) and therefore has more restrictive reporting and access controls.