

**BY ORDER OF THE SECRETARY
OF THE AIR FORCE**

AIR FORCE POLICY DIRECTIVE 16-7

19 FEBRUARY 2014

Operations Support

SPECIAL ACCESS PROGRAMS



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at www.e-Publishing.af.mil for downloading or ordering

RELEASABILITY: There are no releasability restrictions on this publication

OPR: SAF/AAZ

Certified by: SAF/AA
(Mr. Timothy Beyland)

Supersedes: AFPD 16-7, 29 December 2010

Pages: 11

This Directive implements DoD Directive 5205.07, *Special Access Program (SAP) Policy*. It establishes policies and responsibilities for the management, administration, and oversight of SAPs for which the Air Force has cognizant authority (CA), hereafter referred to as SAPs. Air Force shall issue guidance to implement this Directive and DoD Instruction 5205.11, *Management, Administration, Oversight of DoD Special Access Programs*. This directive applies to: all military including members of the Air Force Reserve and Air National Guard, government civilian personnel, contractors and consultants when contract performance depends on access to SAPs, non-DoD U.S. Government Agencies whose personnel, by mutual agreement, require access to SAPs. The terms of any Air Force contract or agreement where SAP access is foreseeable shall require the non-DoD party's compliance with this policy and implementing instructions. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may not be supplemented at any level per Air Force Policy Document (AFPD) 90-1, *Policy Formulation* and AFI 33-360, *Publication and Forms Management*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with *AFMAN 33-363, Management of Records*, and disposed of in accordance with the Air Force Records Disposition Schedule (RDS) located at <https://www.my.af.mil/afrims/afrims/afrims/cfm>. This directive does not supersede any superior authority or supplant specific authorities provide for by Air Force directives or instructions, to the extent they are inconsistent with this Directive. The disclosure provisions in this directive are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector

General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this directive and are controlling.

SUMMARY OF CHANGES

This Directive has been revised to comply with new DoD Directives and Instructions and it must be reviewed in its entirety.

1. Overview. SAPs shall 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 (RDT&E); or when mandated by statute pursuant to DoDD 5205.07. Establishment shall be consistent with Executive Order (E.O.) 13526.

2. Policy.

2.1. The Air Force shall establish a SAP only after formal recommendation to and subsequent approval by the Secretary of Defense (SecDef) or Deputy Secretary of Defense (DepSecDef).

2.2. SAPs shall comply with all applicable statutes, regulations, directives and instructions. All exceptions must be approved, in writing, by the appropriate waiver authority. Approval is required from Security and Special Program Oversight (SAF/AAZ) when policy dictates entry of sensitive information pertaining to SAPs into any unclassified or collateral information systems (IS).

2.3. The Air Force shall establish procedures for all SAPs that allow individuals to report irregularities of fraud, waste, abuse and corruption within secure channels.

2.4. No DoD contractor entity, contractor employee, contractor representative or consultant shall provide SAP material to any members of Congress or congressional staff without DoD Special Access Program Central Office (SAPCO) approval. An employee of the Air Force or an appropriately accessed organization or company is not authorized to brief or provide SAP material to any Congressional Member or staff without the DoD SAPCO approval. SAF/AAZ shall review all reported non-compliance. Failure to comply may be cause for adverse actions, up to and including, revocation of SAP access.

2.5. Members of Congress assigned to designated Defense and Intelligence committees shall be authorized access to SAPs within the respective committee's oversight role, except for waived programs. Unless approved by the SecDef or DepSecDef, only the chair, the ranking minority member and the staff directors of the defense and intelligence committees shall be authorized access to waived SAPs within their committee's respective oversight role.

2.6. Office of Secretary of Defense (OSD) may, on a selective basis, request that the SecAF approve Air Force execution of non-Air Force and non-DoD SAPs (including acting as cognizant authority or executive agent). A memorandum of agreement (MOA) identifying acquisition, contracting, fiscal, legal, manpower, operational and security responsibilities consistent with this AFPD shall be reviewed, at a minimum, by the offices with those

responsibilities. Following the review a recommendation will be made to the SecAF. Offices or organizations executing these SAPs shall comply with the SecAF approved MOA.

2.7. The Air Force shall ensure that SAPs are properly evaluated for potential critical assets that are identified, prioritized and assessed by authorized SAP personnel IAW Defense Critical Infrastructure Program guidance.

2.8. Use of a polygraph examination as an initial SAP access determination requirement shall be specifically approved by the SecDef or DepSecDef as part of the approval of the prospective SAP (PSAP) and consistently applied to all candidates.

2.9. Air Force participation in non-DoD SAPs and joint SAPs with entities of foreign governments shall be governed by MOAs establishing the relationship of the participants regarding security, administration, decision making, and resourcing. MOA terms shall be consistent with national foreign disclosure policy when foreign governments are signatories, and shall follow the disclosure and approval policies established in DoDI 5143.01. The Air Force components shall determine the applicability of DoDD S-5210.36 prior to participating in SAPs or establishing a relationship with entities of foreign governments.

2.10. The SecDef or DepSecDef may approve access of foreign nationals to SAPs. The SecDef or the DepSecDef may make specific delegation of this authority to another official in writing. Foreign nationals shall maintain an equivalent level of clearance and access to classified information based upon commensurate U.S. standards and SAP access agreements negotiated with the foreign government. MOAs for international involvement with SAPs shall be submitted to SAF/AAZ, for review and forwarding to the DoD SAPCO and then to the DepSecDef for approval. Access for foreign nationals not covered in an MOA shall be approved by the SecDef or DepSecDef on a case-by-case basis. All program access requests (PARs) shall be forwarded to SAF/AAZ.

2.11. Treaty compliance requirements, obligations, or constraints shall be considered as an integral part of the policy, planning, operations, and acquisition process for all SAPs.

2.12. The approved Original Classification Authority (OCA) for SAPs are the heads of SAF/AA, The Assistant Secretary of the Air Force for Acquisition (SAF/AQ), The Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (AF/A2), The Deputy Chief of Staff for Operations, Plans and Requirements (AF/A3/5), and The Director, Test and Evaluation (AF/TE). Additional SAP Top Secret OCAs may be designated by the SecAF and additional SAP Secret OCAs may be designated by SAF/AA. This designation shall be done in writing and a copy provided to SAF/AAZ. The approved AF SAP OCA list is maintained by SAF/AAZ. SAP OCAs must receive training in proper classification (including the avoidance of over-classification) and declassification and classification/declassification directives at least once a calendar year. SAP OCAs that do not receive such mandatory training shall have their classification authority suspended by SAF/AA until such training has been taken. SAP OCA training is conducted by SAF/AAZ.

3. Responsibilities.

3.1. The SecAF is responsible for developing and implementing policies and procedures for the management, administration and oversight for SAPs. The SecAF renders the final decision to submit proposals to establish or terminate SAPs, remove programs from special

access controls, alter the scope, category and type of SAP and use Air Force resources to support non-Air Force SAPs.

3.2. The Under Secretary of the Air Force (USecAF) is responsible to represent the Air Force as a member of the SAP Oversight Committee (SAPOC) and, in conjunction with the Vice Chief of Staff (VCSAF), shall designate primary and secondary Senior Review Group (SRG) members.

3.3. The Chief of Staff of the Air Force (CSAF) and VCSAF provide strategic direction for the acquisition, fielding, operations and sustainment of SAPs. The VCSAF shall serve as a member of the SAPOC, and in conjunction with the USecAF, shall designate primary and secondary SRG members. The VCSAF will also serve as the Air Force representative to the Joint Requirements Oversight Council (JROC) for SAPs.

3.4. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) shall:

3.4.1. Serve as the senior security official for the Air Force and is responsible for the efficient and effective implementation of a SAP security program.

3.4.2. Establish an AF SAPCO and designate a Director who is responsible for general oversight for all SAPs.

3.4.3. Assume industrial security oversight responsibilities which shall, at a minimum, meet the standards outlined under the National Industrial Security Program (NISP) and include inspection oversight for those cleared defense contractors executing programs that have been carved-out by SecDef or DepSecDef. SAF/AA is also the responsible senior official to coordinate compliance with current DoD policy on national interest determinations (NIDs).

3.4.4. Serve as the Principal Accrediting Authority (PAA) for all SAP ISs.

3.4.5. Coordinate with SAF/AQ on the nomination of the Director of SAF/AQL, prior to SecAF approval.

3.4.6. Coordinate with AF/A3/5 in the formulation of guidance for Air Force SAP participation in the negotiation, inspection, verification, and compliance support of international arms control and nonproliferation agreements.

3.5. The Auditor General (SAF/AG) is responsible for staffing and maintaining an audit system for SAPs.

3.6. The Assistant Secretary of the Air Force for Acquisition (SAF/AQ) is responsible for acquisition oversight and contracting policy, management and administration of SAPs. SAF/AQ shall nominate an individual for the Director of SAF/AQL, in coordination with SAF/AA, for SecAF approval. Additionally, SAF/AQ shall ensure the appropriate acquisition documents, to include test documents, are provided to AF/A3/5 and SAF/AA for review and assessment of international arms control and nonproliferation implications for SAPs.

3.7. The Chief of Information Dominance and Chief Information Officer (SAF/CIO A6) is responsible to integrate Air Force air, space and cyberspace information and systems into the joint fight. Additionally, as the Chief Information Officer coordinates on SAP policy to ensure compliance with information technology and information assurance statutory requirements.

3.8. The Assistant Secretary of the Air Force for Financial Management and Comptroller (SAF/FM) is responsible for financial oversight policy, management of SAP financial structure, fiscal accountability, audit liaison and financial reporting of SAP resources. Additionally, SAF/FM is responsible for supporting all AF SAP meetings with congressional appropriation committees after coordination with the Special Programs Oversight Committee (SPOC) Executive Secretary and approval by the DoD SAPCO.

3.9. The General Counsel (SAF/GC) is responsible for legal reviews of SAPs to ensure compliance with international law, U.S. statutes, Executive Orders, and DoD and AF directives and instructions. The General Counsel shall be accessed to all SAPs for which the AF participates.

3.10. The Inspector General (SAF/IG) is responsible for performing program security, inspection, investigative, intelligence oversight, and counterintelligence functions for all SAPs and for maintaining a sufficient cadre of special agents, analysts and program security officers (PSOs) to do so. In addition, SAF/IG is responsible for establishing a polygraph and credibility assessment (PCA) program for personnel accessed to SAPs. Through the Air Force Office of Special Investigations (AFOSI), SAF/IG shall appoint a SAP Security Director to execute SAP security responsibilities for all SAPs consistent with the NISP and shall ensure inspections are accomplished for cleared defense contractors supporting programs that have been carved-out by SecDef or DepSecDef.

3.11. The Deputy Chief of Staff for Manpower, Personnel and Services (AF/A1) is responsible for supporting manpower requirements and allocations, as well as personnel assignments for SAPs.

3.12. The Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (AF/A2) is responsible for advocating intelligence requirements, providing substantive intelligence support (i.e. analysis), overseeing acquisition intelligence support (i.e. intelligence missions databases), and providing intelligence oversight for all SAPs. In addition, the AF/A2 shall support AF/TE in the Foreign Material Program (FMP) for SAPs.

3.13. The Deputy Chief of Staff for Operations, Plans and Requirements (AF/A3/5) is responsible for the Air Force implementation of the Joint Capabilities, Integration and Development System (JCIDS), operations planning for all SAPs, and advocating operational requirements for SAPs. AF/A3/5 is the Air Force central authority for activities related to international arms control and nonproliferation agreements and oversees formulation of guidance for Air Force SAP participation in the negotiation, inspection verification, and compliance support of these agreements. AF/A3/5 develops Air Force critical infrastructure strategy, policy and objectives, prepares and implements plans and programs, and advocates plans, operations and funding to Departmental and governmental agencies for SAPs. In addition, AF/A3/5 serves as the Air Force Critical Infrastructure Assurance Officer (AF-CIAO) and the office of primary responsibility for the central management and oversight of the Air Force's critical asset risk management (CARM).

3.14. The Deputy Chief of Staff for Logistics, Installations, and Mission Support (AF/A4/7) is responsible for supporting SAP acquisitions, life cycle sustainment, representing Air Force product support equities, and providing broad policy implementation guidance to Air Force logistics, installations, and mission support activities.

3.15. The Deputy Chief of Staff, Strategic Plans and Programs (AF/A8), is responsible for the Planning, Programming Budgeting and Execution (PPBE) submissions, the strategic basing process for SAPs and the integration (as required) of SAPs into long range strategic planning.

3.16. The Director, Air Force Studies & Analyses, Assessments, and Lessons Learned (AF/A9), is responsible for advising SAP investment decisions by the SPOC with decision-quality analysis.

3.17. The Assistant Chief of Staff, Strategic Deterrence and Nuclear Integration (AF/A10), is responsible for guidance and oversight of SAP activities with nuclear and strategic deterrence equities.

3.18. The Director, Test and Evaluation (AF/TE), is responsible for guidance, direction and oversight of matters affecting test equities for SAP activities. In addition, serve as the lead for the FMP for SAPs.

3.19. MAJCOM Commanders are responsible for establishing a SAP Management Office (SAPMO) and appointing a Director (O-6 or civilian equivalent) as the single focal point within their respective command for coordination, dissemination and reporting of SAP activities and notifying SAF/AAZ of this appointment in writing. MAJCOMs will determine the appropriate staffing and resources necessary for their respective SAPMO.

4. SAP Governance.

4.1. The Air Force shall utilize a resource allocation process that is parallel to the Air Force Corporate process, but is segregated to provide appropriate security. The SPOC shall serve as the senior AF review committee for oversight of resource allocation, acquisition, management, security, and execution of SAPs, including the Military Intelligence Program (MIP). The SPOC is a separate and distinct decision making body from the Air Force Council. At least annually, the SPOC will review the execution and security status of all SAPs. The SPOC review shall be conducted prior to submission of the Program Objectives Memorandum/Budget Estimate Submission (POM/BES) to OSD. SecAF POM/BES approval obtained via the SPOC provides the basis of the Air Force SAP input to the OSD President's Budget (PB) documentation. The SPOC review will also result in the Air Force input to the required OSD review of security administration of DoD SAPs. After the SPOC approves SAP resource levels, no one may make resource adjustments to a SAP without approval of the SPOC Executive Secretary and the SecAF. The SPOC shall:

4.1.1. Review security procedures to ensure the development and application of an appropriate security structure for each SAP.

4.1.2. Eliminate unnecessary duplication of capabilities between SAP, non-SAP, and other DoD programs.

4.1.3. Provide management oversight and guidance for SAPs. This requires reviewing status at program milestones, reviewing audit results, and evaluating other information necessary to assess the progress of a SAP. The SPOC Executive Secretary keeps SPOC members apprised of program status during regular interactions or as required. The SPOC Executive Secretary or appropriate SAP action officers or program managers shall review or provide data as necessary to the SPOC on:

- 4.1.3.1. The portfolio of SAPs.
 - 4.1.3.2. Program objectives and milestones.
 - 4.1.3.3. Current programmatic funding, manpower, facility, and other resource requirements.
 - 4.1.3.4. The existence of any other known programs that may overlap with the SAP being reviewed.
 - 4.1.3.5. The results of internal and external program audits.
 - 4.1.3.6. The programs' current security posture.
 - 4.1.3.7. The justification of retaining SAP status.
 - 4.1.3.8. Discussions of any major security weaknesses and actions to correct those weaknesses, and/or a review of any programs' plan for termination from SAP status.
- 4.2. The Director, SAF/AQL, shall serve as the SPOC Executive Secretary and is the SPOC's representative for all day-to-day SAP activities and represents the SPOC for daily coordination required within the Air Staff and Secretariat on SAP activity.
- 4.3. The SPOC is chaired by the SecAF. Membership in the SPOC is comprised of the following principals: SAF/US, SAF/AA, SAF/AQ, SAF/CIO A6, SAF/FM, SAF/GC, AF/CC, AF/CV, AF/CVA, AF/A1, AF/A2, AF/A3/5, AF/A4/7, AF/A8, AF/A9, AF/A10, and AF/TE. Principals must make every effort to attend. If unable, an appropriately SAP-accessed deputy may substitute, but must be coordinated with the SPOC Executive Secretary in advance. Advisors to the SPOC are SAF/AG, SAF/AAH, SAF/AAZ, SAF/AQC, SAF/FMB, SAF/IG, AF/A8P, and AF/A9F. The SPOC Executive Secretary shall identify SPOC special topic advisors, as required.
- 4.4. The SecAF may designate specific SAPs to be managed outside the SPOC governance structure. A separate agreement, detailing responsibilities for SAP governance, shall be used to document this exception. This agreement must also identify any specific portions of this directive and AFI 16-701 that are also exempt.

DEBORAH LEE JAMES
Secretary of the Air Force

Attachment 1**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References***

- DoDD 3020.40, DoD Policy and Responsibility for Critical Infrastructure, 14 January 2010
- DODI 5100.94, Oversight, Coordination, Assessment, and Reporting of DoD Intelligence and Intelligence-Related Sensitive Activities, September 27, 2011; Incorporating Change 1, October 15, 2013
- DoDD 5101.1, DoD Executive Agent, 3 September 2002, incorporating change 1, 9 May 2003.
- DoDD 5143.01, Under Secretary of Defense for Intelligence (USD(I)), 23 November 2005
- DoDD 5205.07, Special Access Program (SAP) Policy, 1 July 2010
- DoDD S-5210.36, Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government, 6 November 2008
- DoDD 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations, 16 June 1992.
- DoDD 5210.48, Polygraph and Credibility Assessment Program, 25 January 2007
- DoDD 5210.91, Polygraph and Credibility Assessment (PCA) Procedures, 12 August 2010.
- DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs), 6 February 2013
- DoDI 7050.01, "Defense Hotline Program," 17 December 2007
- AFPD 10-24, Critical Infrastructure Program (CIP), 28 April 2006, (Incorporating AFPM, 6 January 2012)
- AFPD 16-6, International Arms Control and Nonproliferation Agreement, and the DoD Foreign Clearance Program, 29 December 2010 (Certified current as of 20 March 2012)
- AFPD 71-1, Criminal Investigations and Counterintelligence, 6 January 2010
- AFPD 90-1, Policy Formulation, 6 October 2010
- AFPD 90-2, Inspector General – The Inspection System, 26 April 2006.
- AFI 10-601, Operational Capabilities Requirements Development, 12 July 2010.
- AFI 14-104, Oversight of Intelligence Activities, 23 April 2012
- AFI 14-111, Intelligence Support to the Acquisition Life-Cycle, 18 May 2012.
- AFI 16-501, Control and documentation of Air Force Programs, 15 August 2006.
- AFI 16-601, Implication of, and compliance with, International Arms Control and Nonproliferation Agreement, 18 February 2011 (Incorporating Change dated 15 November 2011)
- AFI 16-701, Special Access Programs, 1 November 1995.
- AFI 33-360, Publications and Forms Management, 7 February 2013

AFI 71-101, Criminal Investigations, Volume 1, 1 December 1999 (Incorporating Change 1, 17 March 2009)

AFI 99-114, Foreign Material Program, 25 Oct 2002

AFMAN 33-363, Management of Records, 1 March 2008

Adopted Forms

AF Form 847, Recommendation for Change of Publication.

Prescribed Forms

AF Form 673, Air Force Publication/Form Action Request

DD Form 254, Contract Specification Classification Specification

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFOSI—Air Force Office of Special Investigations

BES—Budget Estimate Submission

CA—Cognizant Authority

CARM—Critical Asset Risk Management

DepSecDef—Deputy Secretary of Defense

DoD—Department of Defense

E.O.—Executive Order

FMP—Foreign Material Program

IS—Information System

JCIDS—Joint Capabilities Integration and Development System

MAJCOM—Major Command

MIP—Military Intelligence Program

MOA—Memorandum of Agreement

NISP—National Industrial Security Program

OCA—Original Classification Authority

OSD—Office of Secretary of Defense

PAA—Principal Accrediting Authority

PB—President's Budget

PCA—Polygraph and Credibility Assessment

POM—Program Objective Memorandum

PPBE—Planning, Programming, Budgeting and Execution

PSAP—Prospective Special Access Program

PSO—Program Security Officer

RDS—Records Disposition Schedule

SAP—Special Access Program

SAPCO—Special Access Program Central Office

SAPOC—Special Access Program Oversight Committee

SecAF—Secretary of the Air Force

SecDef—Secretary of Defense

SPOC—Special Programs Oversight Committee

SRG—Senior Review Group

Terms

Carve-out— A provision approved by the Secretary or Deputy Secretary of Defense that relieves DSS of its National Industrial Security Program obligation to perform industrial security oversight functions for a DoD SAP.

Cognizant Authority— The DepSecDef-designated DoD Component Heads, PSAs, or DoD agency heads accountable for management and execution of their respective DoD SAPs.

Memorandum of Agreement (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 Air Force SAPs and DoD or non-DoD SAPs. MOAs define general areas of conditional agreement between two or more parties -- what one party does depends on what the other party does (e.g., one party agrees to provide support if the other party provides the materials). MOAs establish responsibilities for providing recurring reimbursable support should be supplemented with support agreements that define the support, basis for reimbursement for each category of support, the billing and payment process, and other terms and conditions of the agreement. MOAs must be updated or recertified, in writing, every five years.

Oversight— Authority to monitor, review, inspect, investigate, analyze, evaluate and advise an organization's management, operation, performance, and processes through policy, guidelines, instructions, regulations or other structures to maintain compliance and effectiveness within the National Security construct. (This authority does not limit in any way the authority of an Inspector General or others in execution of their lawful duties.)

Oversight Authority— Designated official assigned oversight responsibility for a SAP. Oversight responsibilities include, but are not limited to, endorsing change of category, endorsing apportionment into or de-apportionment from IJSTO, conducting program reviews, endorsing termination or transition plans, ensuring SAPs do not duplicate or overlap, and coordinating SAP annual reports with DoD SAPCO.

Polygraph and Credibility Assessment (PCA)— The overarching term covering programs, research, training, and procedures that employ technologies to assess an individual's truthfulness with the aid of technical devices that measure physiological data or behavioral activity.

Principal Accrediting Authority (PAA)— The principal official with the authority to formally assume responsibility for operating a SAP IS at an acceptable level of risk.

Special Access Program— A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.