BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 16-701
1 NOVEMBER 1995

Operations Support

SPECIAL ACCESS PROGRAMS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: http://afpubs.hq.af.mil. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: SAF/AAZ (Lt Col Leonard E. Patterson)
Supersedes AFI 16-701, 28 Jan 94

Certified by: SAF/AA (Mr. William A. Davidson)
Pages: 27
Distribution: F

The Air Force protects its operational and technological advantages using special access controls. This instruction implements AFPD 16-7, *Special Access Programs*; Executive Order 12356; Title 10, U.S.C. Section 119; and DoD Directive 5205.7. It complements AFPD 31-4, *Information Securit*y, and AFI 31-401, *Information Security Program Management.* It applies to all people and groups involved in Special Access Programs (SAPs), including contractors.

SUMMARY OF REVISIONS

This is the second publication of AFI 16-701, revising the 28 January 94 publication. It clarifies, updates, and streamlines previous guidance on special access programs. A | denotes revised material.

Supersession history: AFR 205-7, Jan 92.

1. Overview of the Air Force Special Access Administrative Process. When normal security methods cannot protect an activity from a known threat, special access controls safeguard operational and technological advantages from potential enemies by limiting access to information about, or observation of, certain weapons, weapon systems, techniques, and operations. DoD, SAF, HQ USAF, and many commands, agencies, and program offices work together in SAPs to create, maintain, modify, and terminate special access controls. The Secretary of the Air Force and Deputy Secretary of Defense set formal SAP policy. A SAP's dynamic oversight feature must be at least equal to normal security programs; justify the need for special access controls by constantly monitoring the specific threat(s) to the program; and require individuals to follow tailored security and operating procedures, public laws, and national policies.

2. Program Oversight. For security reasons, few people have blanket access to SAPs. Among those authorized personnel are members of the Special Access Required (SAR) Programs Oversight Committee (SPOC), the Special Access Program Review Group (SPRG), and selected members of Congress and the

Department of Defense as approved by the DepSecDef. The SECAF chaired SPOC ensures SAP status is justified and that SAPs conform to standards and policy. It reviews program elements, security, and audits of all Air Force SAPs and eliminates duplicate efforts by SAPs and other programs. The SPRG, on the other hand, acts as the Air Force OPR for programmatic and resource review of Special Access Programs.

3. Special Access Programs Categories. For the purpose of sending annual budget reports to Congress, DoD 5205.7 categorizes Special Access Programs as Acquisition (AQ-SAP), Operations & Support (OS-SAP) or Intelligence (IN-SAP).

3.1. AQ-SAP activities are reported to OUSD(A&T)/DSP (AQ-SAP Central Office) because they receive RDT&E, procurement funds, or both.

3.2. OS-SAP activities are reported to DUSD(P)/PS (OS-SAP Central Office) because they do not receive RDT&E or procurement funds, but do protect sensitive operations.

3.3. IN-SAP activities are reported to ASD(C3I)/ODASD(I&S) (IN-SAP Central Office) because they are intelligence funded.

4. Acquisition Planning. Managers of SAPs impacted by DoD acquisition directives (5000.x series) must consider guidelines specifically tailored to SAPs.

4.1. Contracting in Special Access Programs. SAPs conform to contracting regulations, including the Federal Acquisition Regulation (FAR), Defense FAR Supplement (DFARS), and Air Force FAR Supplement (AFFARS). These regulations reflect the laws, Executive Orders, and OSD policy applying to all DoD acquisitions except those specifically exempted. In addition, major command regulation supplements and other regulations further guide contracting offices. Clearly, SAP acquisition offices may not be able to conform to some regulations without compromising national security or violating security restrictions. Some regulations already provide sufficient exceptions for national security or classified information. Other deviations may require case-by-case waivers.

4.1.1. SAF/AQCF is the Air Force focal point for FAR, DFARS, and AFFARS deviations. SAP acquisition offices submit deviation requests to the SAF/AQC contracting staff officer located in SAF/AQL for staffing and approval. Deviation requests must be formatted IAW DFARS 201.402 and AFFARS 5301.402.

4.2. Designating Carve-Out Contracts. "Carve-out contracting" removes a program from the security oversight of the Defense Investigative Service's Defense Industrial Security Program. The DoD Information Security Regulation (DoD 5200.1R) authorizes carve-out contracting only for SAPs that meet exceptionally stringent security criteria. Chapter XII of DoD 5200.1R describes the criteria for carve-out status. Only the Secretary or Deputy Secretary of Defense can approve carve-out contracting. Program managers will request carve-out contracting with the request for SAP approval to the Deputy Secretary of Defense and revalidate carve-out procedures annually.

4.2.1. Using the DD Form 254, DoD Contract Security Classification Specification. Activities sponsoring a SAP with contractor support use DD Form 254, classified if necessary, when creating a carve-out from DIS. DD Forms 254 must include requirements for contractor(s) to identify specific program locations (such as a safes, rooms, buildings, plants, etc.) which are a "carve-out" to the program's CSA. Send a copy of each DD Form 254 to the proper DIS security office, except when a SAP needs extra protection. In this case, forward DD Form 254 to SAF/AAZ, who notifies DUSD(P) or DIS.

5. Relationships Among Special Access Security Controls, Procedures, Activities, Programs, and Other Security Systems. Executive Order 12356, *National Security Information,* as implemented by Information Security Oversight Office (ISOO) Directive No 1; DoD 5200.1R/AFPD 31-4/AFI 31-401; and DoDD O-5205.7, implements special access controls. These controls provide extraordinary protection by: keeping personnel access to the minimum needed to meet program goals; setting investigative or adjudicative criteria for persons seeking access; naming officials who determine whether cleared people have a need-to-know; using access lists and registered unclassified nicknames (and, in some cases, classified code words) to identify information needing additional protection; security guides and procedures specifically tailored for certain information and equipment; and supporting and overseeing infrastructures. Security controls protect a given activity. A special access program is the protected activity. The Secretary or Deputy Secretary of Defense formally approves, in writing, these legally defined programs and annually reports on them to Congress. Each Air Force SAP and each SAP the AF operates for other agencies or activities must be formally registered with SAF/AAZ, the Air Force SAP Central Office (SAPCO). SAPs containing Sensitive Compartmented Information (SCI) or Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI) may have other security control systems, such as SCI and SIOP-ESI. For example, SAPs must obtain approval to introduce the SAP into a Sensitive Compartmented Information Facility (SCIF) from HQ 497 IG/INS and also negotiate a security agreement with HQ 497 IG/INS. Since SAPs in SCIFs are usually a tenant, SCI directives govern SCI protection. These additional security control systems apply only to that specific compartmented information. The term SAP, often substituted for "Special Access Required (SAR)", may describe the security control system, the entire effort, and in some cases certain budget information.

6. The SAP Administration System Concept. Senior management uses the SAP to increase the security of information about an activity. Only "core secrets" have special access controls; in an unacknowledged program, its very existence is a core secret and all information relating to the program may be protected with special access controls. Normal security controls, classification, and handling systems protect other information. Examples of activities protected with special access controls might include a technology breakthrough or exploitation of an enemy's weakness. A SAP could also fix a US weakness or protect extremely sensitive operations.

6.1. SAP Initiation and Approval Procedures. An Air Force office wanting to establish a SAP sends a recommendation through command channels to the HQ USAF or SAF office responsible for the activity. At a minimum, the request must contain the information in **Attachment 2** and the approval memoranda (**Attachment 3**) for the Secretary of the Air Force to sign. Mark all documentation with the proposed special access classification markings (see **6.1.1.**paragraph.) or other information to reflect minimum access required. Coordinate the request with the responsible DCS, ACS, or Secretariat office and include at least: HQ USAF/PE, to evaluate funding and manpower need; SAF/AA, to review security plans; SAF/GC, to review legal issues; SAF/FM, to review funding; and HQ USAF/IN, to review programs with SCI material or needing the intelligence community to participate and to approve the overall threat assessment (see **6.1.1.**paragraph.). Then send request through HQ USAF/CC and SAF/US to SAF/OS for the final decision before forwarding it to OSD. The responsible Air Staff office will prepare proposed approval memoranda for Secretary of the Air Force signature. SAF/AAZ routes the approval packages through the appropriate OSD Central Office to the Deputy Secretary of Defense.

6.1.1. A thorough, current threat assessment constitutes the basis for applying and maintaining special access controls to a program. In the absence of a threat, special access controls are inappropriate. Likewise, changing threats may deem special access controls no longer necessary. Threat assessments must consider both the system threat and the intelligence threat. System threats prepared by USAF/IN generally apply to AQ-SAPs and describe the threat to be countered by the weapon system. The focus of the system threat is to identify current and projected capabilities that an adversary could use to defeat, destroy, degrade, or deny the effectiveness of a proposed concept or system. The intelligence threat, on the other hand, is normally assessed by AFOSI and describes the susceptibility that program information will be compromised through foreign intelligence activities. These activities include Signals Intelligence (SIGINT), Imagery Intelligence (IMINT), Human Intelligence (HUMINT), Measurement and Signatures Intelligence (MASINT), and Open Source Intelligence (OSINT).

6.1.2. Prospective Special Access Programs (PSAP). During the SAP approval process, you may protect information with Prospective Special Access Programs (PSAP) procedures. SAF/AAZ gives PSAP status in a formal memorandum sent to the program office. Unless the PSAP gains formal SAP status, or the protected program ends or is reclassified, the PSAP automatically ends after 180 days. A PSAP's only purpose is to protect information until the SAP staffing is completed.

6.2. Air Force Participation in a Program Directed by Another DoD Component or Another Agency. Any request for Air Force participation in or support of another DoD Component or Agency's SAP must be made through SAF/AAZ. At a minimum, the request must contain a proposed Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) and the information described in **Attachment 4** SAF/AAZ will ensure the responsible Air Force office reviews the recommendation and coordinates it with the responsible DCS, ACS, or Secretariat office, as well as SAF/OS, SAF/US, HQ USAF/CC, USAF/CV, SAF/GC, SAF/AA, SAF/FM and HQ USAF/PE (for SAPs proposing to use Air Force funds or manpower), and HQ USAF/IN (for all programs with SCI material or having intelligence community participation). SAF/FM will also coordinate on those programs where Air Force funding is not involved but other component/agency funding flows through Air Force mechanisms. If the agreement originates outside DoD, the Air Force must notify the Deputy Secretary of Defense.

6.3. Changes in SAP Controls. SAP managers notify Congress before they make significant changes in SAPs, such as termination, discarding controls, regrading to collateral, and public announcement. Program managers prepare notification packages in advance and forward them through SAF/AAZ to the Deputy Secretary of Defense. Contact SAF/AAZ for additional information.

7. SAP Access. DoD and other Executive Agency and legislative members or employees may require SAP access to meet their support or oversight responsibilities. Some may need only administrative information (such as printing plant personnel and administrative staff) while others (such as the Air Force SPOC and the Joint Staff's Joint Requirements Oversight Committee (JROC)) may need detailed briefings to fully understand the impact of their actions on a SAP. People outside the Air Force (i.e., DoD/IG, other services, etc.) normally send a Program Access Request (PAR) memo to the SAPCO (SAF/AAZ), who forwards it to the program manager to determine the need-to-know and access level. **Attachment 5** describes the specific policies and procedures for granting SAP access to legislative members and employees. Certain organizations, such as the JROC, have established billet structures (as found in JSI 5220.02) to identify personnel needing access because they routinely work SAP issues. Such billet structures are not blanket access approvals nor do they give all persons in the billets access to any or all SAPs. Access is given on a case-by-case, need-to-know basis.

7.1. Ensuring Personnel Security for Access to SAPs. The minimum security clearance level for access to SAP information is a Secret clearance based on a National Agency Check with Credit Check (NACC). The NACC must be no more than five years old. Access control procedures are strictly followed and to gain access, personnel must accept, in writing, specific restrictions and liability for unauthorized disclosure. Additionally, personnel may undergo separate access adjudication procedures beyond basic security clearance. Persons requiring access to one or more SAPs may be subject to periodic counterintelligence scope polygraph examinations, within the limits set by Congress or the Office of the Secretary of Defense. Commanders and supervisors continually evaluate all personnel with access to SAP information. Follow the continuing evaluation requirements found in AFI 31-501 and in SAP Security/Classification Guides.

7.1.1. Special Handling Procedures. SAP materials require enhanced security measures by all persons generating or handling such materials. To ensure proper handling of these types of materials, the procedures and practices listed in **Attachment 6** apply to all SAPs.

7.2. Administrative Recourse. The Air Force follows DoD policies for administrative recourse for all SAP personnel security and access decisions. If reports on a candidate are unfavorable, a central adjudication office sends a letter to the applicant's security staff stating access is denied, suspended, or limited. A properly marked, sealed letter for unopened delivery to the candidate is included. When consistent with national security, the letter explains the action; gives the candidate 30 days to request information about the action; and states that the candidate may submit clarifying, rebutting, mitigating, or explanatory information. If, after reviewing the new information, the judgment remains unfavorable, the candidate receives notification and an explanation of other appeal procedures.

8. Responsibilities of Offices Associated with SAPs.

8.1. The Administrative Assistant to the Secretary of the Air Force (SAF/AA) serves as the Senior Security Official of the Air Force, responsible for policies implemented by this instruction within the Department of the Air Force and Air Force Contractors. SAF/AAZ, the Air Force SAP Central Office (SAPCO):

- Maintains the Air Force central registry for all Air Force SAPs.
- Administers oversight and implementation of Air Force SAP security
- Helps SAP security managers develop security plans.
- Coordinates, as the Air Force SAPCO, external oversight and support by Department of Defense Inspector General (DoD/IG), DUSD(P), DIS, General Accounting Office (GAO), and other US government agencies.
- Forwards packages for creating and disbanding SAPs to DEPSECDEF.
- Coordinates annual reviews of each Air Force SAP.
- Supports or helps obtain specialized support in numerous areas for particularly sensitive programs. **Attachment 7** lists some of the support available.
- Operates and maintains the Air Force database of codewords and nicknames.

8.2. The Assistant Secretary of the Air Force for Financial Management (SAF/FM):

- Oversees the financial structure, budget, cost, accounting controls, execution, and comptroller functions (including audit liaison) for SAPs.
- Approves special funding techniques for programs funded by other than normal means.

8.3. The Office of the Assistant Secretary of the Air Force for Acquisition (SAF/AQ):

- Oversees AQ-SAPs.
- Through the Security Director, publishes classification guidance to ensure coherent security throughout life of programs.
- Oversees research, technology base, system technical issues, and systems development related to SAPs.
- Provides program milestone guidance and support.
- Oversees polices for SAP production, contract, and business issues.

8.4. The Office of the General Counsel (SAF/GC) has access to all SAPs and reviews them for compliance with law, Executive Order, and regulation before their approval.

8.5. The Air Force Inspector General (SAF/IG) has access to Air Force SAPs as needed to perform statutory responsibilities and provide investigative, counterintelligence, and security support to selected SAPs.

8.6. The Auditor General (SAF/AG):

- Staffs and maintains an audit system for SAPs with properly cleared and qualified personnel.
- Provides audit service to SAPs and recommends corrective actions.

8.7. The Deputy Chief of Staff for Programs and Evaluation AF/PE:

- Is the focal point for all SAP manpower issues.
- Acts as the single contact for all Biennial Planning, Programming, and Budgeting Systems submissions for SAPs.

8.8. The Assistant Chief of Staff, Systems for Command, Control, Communications &Computers

(HQ USAF/SC) acts as the communications and computer system focal point for selected SAPs.

8.9. The Deputy Chief of Staff for Plans and Operations (HQ USAF/XO):

- Oversees OS-SAPs.
- Oversees the requirements process, including developing and staffing Mission Need Statements and Operations Requirements Documents, related to SAPs.
- Provides operational requirements inputs at the earliest opportunity for research, technology base, system technical issues, system security, and systems development related to SAPs.

8.10. The Assistant Chief of Staff/Intelligence (HQ USAF/IN):

- Reviews all SAPs involving SCI material or requiring intelligence community participation.
- Oversees IN-SAPs.
- Supports special access program managers in preparing system threat assessments.
- Approves overall threat assessments for SAPs.

9. Responsibility for SAP Security. The program manager or commander is responsible for security and:

- Monitors personnel, financial resources, and facilities to support the SAP.
- Implements OPSEC measures needed to support the program and ensures an aggressive and tailored security education program for all participants.
- Ensures all prime contractor and sub-contractor facilities are inspected by the cognizant security agency. For AF/IN SAPs in SCIFs, the frequency of inspection will be determined by the CSA based on local threat, problems identified in the past, major modifications, and sensitivity of the program as defined in DCID 1/21, Physical Security Standards for Sensitive Compartmented Information Facilities.
- Ensures a trained security manager, whose primary responsibility is security, is assigned to the program and provides the resources for each program's needs. The resources may belong to the SAP exclusively or come from other activities and organizations.
- Ensures a tailored security and classification guide is published for each SAP. The guide explains all program security needs and procedures associated with the program and gives specific classification and regrading guidance. It also explains how to report fraud, waste, and abuse (FWA) without violating security agreements and procedures. Each person participating in the program is taught to report FWA properly.
- Ensures that an arms control managed access plan is available for implementation, if appropriate. This plan will be IAW Air Force and MAJCOM arms control compliance plans for all arms control agreements.

10. Reporting Requirements. SAF/AAZ compiles and submits annual SAP reports (DoD Report Control Symbol: DD-C3I(A)1605) to OSD Central Offices, which send them to Congress. Annual SAP reports serve as the vehicle for annual DEPSECDEF revalidation and SAP approval. By 1 December of each year, program managers send SAF/AAZ a report in the format given in **Attachment 8** Program managers also send SAF/AAZ by 31 December of each year a separate security report (SAP Summary) per DoD 5200.1R and the instructions given in **Attachment 9** SAF/AAZ compiles these reports and sends them to DUSD(P). Program managers also report program nicknames to SAF/AAZ whenever they change.

11. Handling Program Artifacts. The program manager must properly screen classified or sensitive unclassified objects such as test equipment, test fixtures, prototype systems, models, and associated technical information and files for intrinsic or historical value. Actions the program manager considers include reviewing the objects' classification, destroying it, giving it to the contractor or other DoD organizations to keep or destroy, and sending it to a museum or a secure storage site.

11.1. SAF/AAZ coordinates and provides specific instructions for disposing of classified or sensitive unclassified SAP artifacts. Contact SAF/AAZ before disposal.

WILLIAM A. DAVIDSON
Administrative Assistant

Attachment 1

GLOSSARY OF REFERENCES, ABREVIATIONS, ACRONYMS, AND TERMS

References

NOTE:

Be sure to use the most current versions of these documents.

Executive Order 12333, "*United States Intelligence Activities*," December 1981

Executive Order 12356, "*National Security Information*," 1 April 1982

Public Law 95-452, "*Inspector General Act of 1978,*" as amended

ISOO Directive No. 1, "*National Security Information*," June 1986

DCI Directive 1/19, "*Security Policy for SCI,"* 19 February 1987

DCI Directive 1/21, "*Physical Security Standards for SCIFs," 3*0 January 1994

DoD Directive 5000.1, "*Defense Acquisition*," February 23, 1991

DoD Instruction 5000.2, "*Defense Acquisition Management Policies Procedure*s," February 23, 1991 (including Air Force Supplement 1)

DoD Directive 5106.1, "*Inspector General of the Department of Defense*," 14 March 1983

DoD Directive 5106.3, "*Inspector General, Department of Defense, Inspection Program*," 26 July 1989

DoD Directive 5137.1, "*Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)*," 2 April 1985

DoD Directive 5148.11, "*Assistant to the Secretary of Defense (Intelligence Oversight),"* 1 December 1982, as amended by Changes 1 and 2

DoD Directive 5200.1, "*DoD Information Security Program*," 7 June 1982

DoD Manual 5200.1M(Draft), "*Acquisition Systems Protection Program*," July 1993

DoD Directive 5200.2, "*Personnel Security Program*," January 1989

DoD Manual 5200.22M, "*Industrial Security Manual*," January 1991

DoD Directive 5200.5, "*Communications Security (COMSEC)*," 6 October 1981

DoD Directive O-5205.7, "*Special Access Programs (SAP) Policy*," 4 January 1989

DoD Directive S-5200.19, "*Control of Compromising Emanations*," 10 February 1968, as amended by Change 1 and Transmittal 68-3

DoD Directive S-5210.36, "*Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government*," 10 June 1986

DoD Directive 5200.28, "*Security Requirements for Automated Information Systems (AISs)*," 21 March 1988

DoD Directive 5205.2, "*DoD Operations Security Program*," 7 July 1983

DoD Directive 5230.11, "*Disclosure of Classified Military Information to Foreign Governments and International Organizations,*" 31 December 1984

DoD Directive 5240.1, "*DoD Intelligence Activities*," 25 April 1988, as amended by Change 1

DoD Directive 5240.12, "*DoD Intelligence Commercial Activities (ICAs)," 2 December 1992*

DoD Directive 5240.2, "*DoD Counterintelligence*," 6 June 1983

DoD Directive 7050.5, "*Coordination of Remedies for Fraud and Corruption Related to Procurement Activities*," 27 June 1989

DoD Instruction 5505.2, "*Criminal Investigations of Fraud Offenses*," 6 November 1987

DoD Instruction 7050.3, "*Access to Records and Information by the Inspector General, Department of Defense*," 9 November 1984

DoD Manual 7750.5, "*DoD Procedures for Management of Information Requirements*," November 1986, as amended by Change 1

DoD Regulation 5200.1R, "*Information Security Program Regulation*," 28 April 1987, as amended by Change 1

DoD Regulation 5200.2R, "*DoD Personnel Security Programs*," January 1987

DoD Regulation 5210.48R, "*Polygraph Program*," January 1985

DoD Regulation 5220.22R, "*Industrial Security Regulation*," December 1985

Secretary of Defense Memorandum, "*Access by the DoD Inspector General to Special Access and Other Sensitive Programs*," 17 June 1988

USAFINTEL 201-1, "T*he Security, Use, and Dissemination of Sensitive Compartmented Information (SCI)*," 1 May 1990

Abbreviations and Acronyms

ACS—Assistant Chief of Staff

AF—Air Force or Department of the Air Force

AIA—Air Intelligence Agency

AFMC—Air Force Materiel Command

AFOSI—Air Force Office of Special Investigations

AFOTEC—Air Force Operational Test and Evaluation Center

AIS—Automated Information System

BI—Background Investigation

ASD—Assistant Secretary of Defense

ASPO—Acquisition Systems Protection Office

BPPBS—Biennial Planning, Programming, and Budgeting System

C2—Command and Control

C2W—Command and Control Warfare

C3—Command, Control, and Communications

C3I—Command, Control, Communications, and Intelligence

C4—Command, Control, Communications, and Computers

CI—Counterintelligence

CINC—Command-in-Chief

CJCS—Chairman of the Joint Chiefs of Staff

COMPUSEC—Computer Security

COMSEC—Communications Security

CONOPS—Concept of Operations

COTS—Commercial Off-the-Shelf

CSA—Cognizant Security Authority

CSAF—Chief of Staff of the Air Force

DAB—Defense Acquisition Board

DCAA—Defense Contract Audit Agency

DCI—Director of Central Intelligence

DCS—Deputy Chief of Staff

DIA—Defense Intelligence Agency

DIS—Defense Investigative Service

DoD—Department of Defense

DoD(IG)—Department of Defense (Inspector General)

DPG—Defense Planning Guidance

DSN—Defense Switched Network (formerly AUTOVON)

DT&E—Development Test and Evaluation

DUSD(P)—Deputy Under Secretary of Defense (Policy)

EEFI—Essential Elements of Friendly Information

EPITS—Essential Program Information, Technologies, and/or Systems

EMSEC—Emission Security

EP—Electronic Protection

FBI—Federal Bureau of Investigation

FCT—Foreign Comparative Test

FOA—Field Operating Agency

FOC—Full Operational Capability

FWA—Fraud, Waste, and Abuse

FY—Fiscal Year

FYDP—Five Year Defense Plan

GAO—General Accounting Office

HQ AFOTEC—Headquarters, Air Force Operational Test and Evaluation Center

HQ USAF—Headquarters, United States Air Force

ILSP—Integrated Logistics Support Plan

IOC—Initial Operational Capability

ISOO—Information Security Oversight Office

JCS—Joint Chiefs of Staff

JROC—Joint Requirements Oversight Council

MAJCOM—Major Command

MNS—Mission Need Statement

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

NFIP—National Foreign Intelligence Program

OPM—Office of Personnel Management

OPR—Office of Primary Responsibility

OPSEC—Operations Security

ORD—Operational Requirements Document

OSD—Office of the Secretary of Defense

OT&E—Operational Test and Evaluation

OUSD(A&T)—Office of the Under Secretary of Defense (Acquisition & Technology)

PB—President's Budget

PEO—Program Executive Officer

PM—Program Manager

PMD—Program Management Directive

POC—Point of Contact

POM—Program Objective Memorandum

PSAP—Prospective Special Access Program

R&D—Research and Development

RDT&E—Research, Development, Test and Evaluation

SAF—Secretary of the Air Force

SAP—Special Access Program

SAPCO—Special Access Program Central Office

SAR—Special Access Required

SCI—Sensitive Compartmented Information

SECDEF—Secretary of Defense

SP—Security Police

SPO—System Program Office

SPOC—Special Access Required Programs Oversight Committee

SPRG—Special Programs Review Group

SSBI—Single Scope Background Investigation

SSEM—System Security Engineering Management (or Manager)

STA—System Threat Assessment

STAR—System Threat Assessment Report

TBD—To Be Determined

TEMP—Test and Evaluation Master Plan

TIARA—Tactical Intelligence and Related Activities

VCJCS—Vice Chairman of the Joint Chiefs of Staff

Terms

Terms— This glossary helps the reader understand some terms that describe SAPs. Readers may also find these publications helpful: Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," 1 December 1989, and AFM 11-1, "Air Force Glossary of Standardized Terms," They contain standard terms and definitions that the Department of Defense and Air Force use.

Appropriation Codes— A fund authorization set up by an act of Congress that permits a department or other government agency to obligate the Federal Government to pay for goods and services. Appropriations and their budget codes are as follows:

-3010	Aircraft procurement funding
-3020	Missile procurement funding
-3080	Other procurement funding
-3300	Military construction funding
-3400	Operations and maintenance funding
-3500	Military personnel funding

-3600 Research, Development, Test, and Evaluation funding

(AFP 172-4)

Automated Information System (AIS)— A combination of information, including computer and telecommunications resources and other information technology, as well as personnel resources, which collect, record, process, store, communicate, retrieve, and display information. (DoD Directive 7920.1)

Carve-Out— A classified contract issued in connection with a SAP. A carve-out eliminates or reduces conventional oversight duties.

Central Office— SAF/AAZ is the Air Force SAP Central Office that coordinates the management review, oversight and control of SAPs.

Communications Security (COMSEC)— The protection resulting from all measures designed to deny unauthorized persons valuable information, which experts in electronics or telecommunications might be able to find. Some measures lead unauthorized persons to an incorrect interpretation of the information.. COMSEC includes:

Cryptosecurity— The component of COMSEC that results from the providing and properly using technically sound cryptosystems. .

Emission Security (EMSEC)— The component of COMSEC which results from all measures taken to deny unauthorized persons valuable information that might be derived from intercept and analysis of compromising emanations from cryptoequipment and telecommunications systems.

Physical Security— The component of COMSEC that results from all physical measures necessary to safeguard classified equipment, material, and documents from access or observation by unauthorized persons.

Transmission Security (TRANSEC)— The component of COMSEC that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. (Joint Publication 1-02)

Concept of Operations (CONOPS)— A verbal or graphic statement, broadly outlining a commander’s assumptions about or purpose of an operation or series of operations. The concept of operations frequently is embodied in campaign plans and operation plans; in the latter case, particularly when the plans cover a series of connected operations to be carried out simultaneously or in succession. The concept is designed to give an overall picture of the operation. It is included primarily for additional clarity of purpose. Frequently, it is referred to as commander’s concept. (Joint Publication 1-02)

Core Secrets— Any item, process, strategy, or element of information, the compromise of which would result in unrecoverable failure.

Information Security— The result of any system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information that executive order or statute protects. (DoD 5200.1-R/AFR 205-1)

Need to Know— A security criterion that requires the custodians of classified information to establish, prior to disclosure, that the intended recipient must have access to the information to perform his or her official duties.

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

(Joint Publication 1-02)

Operations Security (OPSEC)— A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to:

- Identify actions that adversary intelligence systems can observe.
- Determine which indicators hostile intelligence systems might obtain and then interpret or piece together to discover critical information useful to adversaries.
- Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.
- (Joint Publication 1-02)

Physical Security— The part of security concerned with physical measures designed to safeguard personnel; prevent unauthorized access to equipment, installations, material, and documents; and safeguard them against espionage, sabotage, damage, and theft. (Joint Publication 1-02)

Program Office— The office that manages, executes, and controls a SAP in a DoD component.

Program Protection Plan— A comprehensive protection and technology control management tool established for each defense acquisition program to identify and protect classified and other sensitive information from foreign intelligence collection or unauthorized disclosure.

Sensitive Compartmented Information (SCI)— All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established.

Special Access Program (SAP)— Under the authority of Executive Order 12356 and as implemented by the Information Security Oversight Office (ISOO) Directive No. 1, any program created by an agency head whom the President has designated in the Federal Register to be an original TOP SECRET classification authority that imposes "need-to-know" or access controls beyond those the DoD normally requires for access to CONFIDENTIAL, SECRET, or TOP SECRET Information. Such a program includes, but is not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine need-to-know; or lists of persons who actually have a need-to-know.

Special Access Required (SAR) Programs Oversight Committee (SPOC)— The senior Air Force Review Committee for overseeing resource allocation, acquisition, management, security, and execution of Air Force Special Access Programs (Excluding NFIP). The Secretary of the Air Force approves a Charter which describes the organiztion, composition, and functions of the SPOC.

Special Program Review Group (SPRG)— The committee responsible for developing the Air Force SAR programs resource requirements, including the Program Objective Memorandum, Budget Estimate Submission, and the President’s Budget.

Attachment 2

SPECIAL ACCESS PROGRAM APPROVAL REQUEST REQUIREMENTS

A2.1. Identify the Air Force OPR for requested program.

A2.2. Provide the classified codeword and the unclassified nickname of the program and its subelements (DoD 5200.1R/AFR 205-1, appendix C).

A2.3. Describe the relationship, if any, to the other Special Access Programs (SAP) in the Department of the Air Force, Department of Defense (DoD), or other government agencies.

A2.4. Explain the rationale for establishing the SAP, including the reason why normal security management and safeguard procedures for classified information are inadequate, a summary of the validated threat, and how the special security requirements will defend against it.

A2.5. Estimate how many persons in the DoD, other government agencies, Congress (including staffers), and contractors will require special access.

A2.6. Summarize in writing program security needs for:

A2.6.1. Security professionals (security police (SP), Air Force Office of Special Investigations (AFOSI), 497th Intelligence Group/INS (497 IG/INS), etc.)

A2.6.2. Security and personnel investigation .

A2.6.3. Special physical, computer, communications, or TEMPEST security.

A2.7. Tell who is responsible for:

A2.7.1. Program security policy.

A2.7.2. Industrial security inspections (DIS or program security personnel)..

A2.7.3. Programs using, storing, and producing Sensitive Compartmented Information must coordinate and obtain approval from HQ 497 IG/INS for the introduction of a SAP into a SCIF.

A2.8. Describe procedures for:

A2.8.1. Establishing the program security, classification, and industrial security guides.

A2.8.2. Conducting an annual review to determine if persons with need-to-know status should have continued access.

A2.8.3. When possible, taking classified information out of lengthy documents and handling it separately, so distribution is easier.

A2.8.4. Marking the cover and first page of documents to show they contain SAP information.

A2.8.5. Handling, opening, and distributing SAP materials by clerical, mail, and telecommunications personnel.

A2.8.6. Sending electronically transmitted messages.

A2.9. Identify the future Year Defense Plan funds or estimate the funds a new program needs.

A2.10. Identify the HQ Air Force official to contact about the program (last name, first name, office symbol, and telephone number).

A2.11. Identify budget resources by appropriation, program element, and fiscal year.

Attachment 3

SPECIAL ACCESS PROGRAM APPROVAL MEMORANDA

Example Only This Page UNCLAS
SECRET-(NICKNAME) SPECIAL ACCESS REQUIRED
SECRETARY OF THE AIR FORCE (LETTERHEAD)
EXECUTIVE SUMMARY

MEMORANDUM FOR THE DEPUTY SECRETARY OF DEFENSE

THROUGH: UNDER SECRETARY OF DEFENSE (ACQUISITION AND TECHNOLOGY)/DIRECTOR OF SPECIAL PROGRAMS (for an AQ-SAP)
DEPUTY TO THE UNDER SECRETARY OF DEFENSE (POLICY) FOR POLICY SUPPORT (for an OS-SAP)
ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS & INTELLIGENCE (for an IN-SAP)

FROM: Secretary of the Air Force

SUBJECT: Initiating/Disbanding (Nickname) as an Air Force Special Access Program (SAP)(U)

PURPOSE: (U) ACTION--To obtain DEPSECDEF approval to initiate (Nickname) and signature on notification letters.

DISCUSSION: (S/SAR) The Air Force recommends approval of (Nickname) as an Air Force SAP, (if required) carved-out from the cognizance of the Defense Investigative Service. The program is designed to limit the likelihood of the US Government losing its technological lead in (Generalized Purpose Statement). The SAP management structure will protect special access information while in transition to collateral (non-special access) levels. (Relationships, if any, with other Programs. Changes to other Programs, etc.) Carve-out status is justified by the need to tightly control extremely sensitive information; a dedicated security infrastructure will provide support.
Atch 2 describes the program and its funding.

RECOMMENDATION
(S/SAR) That DEPSECDEF approve/disband (nickname) and sign notification letters at Atch 1.

DEPSECDEF DECISION
____________________ Approved
____________________ Disapproved
____________________ Other:___________________________________

2 Atch
1. Congressional Notification Letters (4) (6 for IN-SAP)(S/SAR)
2. Program Description w/Atch (S/SAR)

Classified by Multiple Sources
Declassify OADR

SECRET-(Nickname)-SPECIAL ACCESS REQUIRED
Example only - this page UNCLAS

Deputy Secretary of Defense Letterhead

SAMPLE

Honorable John B. Doe
Chairman, Committee on (Name of Committee)
House of Representatives
Washington, D.C. 20515-0000

Dear Mr. Chairman:

(X/XX) Consistent with Section 119(f) of Title 10, United States Code, this is to notify you that I have approved initiation of the Special Access Program named (Nickname) as proposed by the Secretary of the Air Force, effective 30 days from receipt of this letter.

(X/XX) This program protects extremely sensitive information related to ____________
____

(U) Funds for this Special Access Program have been approved for obligation no earlier than 30 days after receipt of this letter.

Sincerely,

(DepSecDef)

cc:
Honorable Patricia B. Doe
Ranking Minority Member

Classified by:________________
Declassify On:________________

CLASSIFICATION

Enclosure 1 to attachment 3

Deputy Secretary of Defense Letterhead

SAMPLE

Honorable John B. Doe
Chairman, Committee on (Name of Committee)
House of Representatives
Washington, D.C. 20515-0000

Dear Mr. Chairman:

(X/XX) Consistent with Section 119(c)(1) of Title 10, United States Code, this is to notify you that I have approvec the (change in classification/declassification) of the Special Access Program named (Nickname). This program will be (declassified/reclassified) as proposed by the Secretary of the Air Force, effective no later than 14 days from the date of this letter. After that date the program will be (unclassified/classified) at the (classification) level.

(X/XX) Special Access Program (Nickname) is being (declassified/reclassified) because

____

____.

A public announcement of this change in classification (is/is not) planned. (The announcement will take place on or about_________________________.

Sincerely,

(DepSecDef)

cc:
Honorable Patricia B. Doe
Ranking Minority Member

Classified by:_______________
Declassify on:_______________

CLASSIFICATION

Enclosure 2 to attachment 3

Attachment 4

PARTICIPATION IN A SAR PROGRAM DIRECTED BY ANOTHER DOD COMPONENT OR AGENCY

A4.1. Identify the activity requesting Air Force support.

A4.2. Identify the Air Force activity who will act as Air Force OPR for the program.

A4.3. Provide the classified codeword, if any, and unclassified nickname of the program and its subelements.

A4.4. Describe the relationship, if any, to other SAPs in the Air Force, DoD, or other government agencies.

A4.5. Summarize the program briefly, including the MOU or MOA and outlining extent of Air Force involvement in support of the program.

A4.6. Estimate the number of Air Force personnel who will be granted access to the program.

A4.7. Summarize program security requirements, to include:

A4.7.1. Who manages overall program security (Air Force or directing agency).

A4.7.2. What specific security requirements does the directing agency impose?

A4.7.3. Whether DIS, the directing agency, or the Air Force will conduct industrial security inspections.

A4.7.4. Whether the approval package includes attachments, such as security classification guides or other guidance applicable to the program.

A4.7.5. Whether programs using, storing, or producing Sensitive Compartmented Information have been coordinated with HQ 497 IG/INS and approved for introducing a SAP into a SCIF.

A4.7.6. Any special physical security, communications security, computer security, or TEMPEST requirements imposed by the directing agency.

A4.8. Identify whether the directing agency or the Air Force provides funds.

A4.9. Identify the HQ Air Force official to contact about the program (last name, first name, office symbol, and telephone number).

Attachment 5

POLICIES AND PROCEDURES ON ACCESS TO SAP INFORMATION FOR EMPLOYEES OF THE LEGISLATIVE BRANCH

A5.1. Purpose . This attachment amplifies the DoD policy on access to information protected with Air Force or joint SAPs for employees of the Legislative Branch and details procedures on how access to program information may be requested.

A5.2. Scope. These policies and procedures for Air Force SAPs apply to Legislative Branch and the General Accounting Office (GAO) employees. These procedures do not apply to SAPs initiated under the authority of the Director of Central Intelligence (DCI) or other Executive Branch departments and agencies.

A5.3. Air Force Policy:

A5.3.1. Only permanent professional staffs of congressional defense committees and selected intelligence committees, and employees of the GAO who have a minimum of a SECRET clearance and a need-to-know gain access to Air Force SAPs, while serving in an official capacity for the following:

A5.3.1.1. DoD authorization or appropriation legislation.

A5.3.1.2. DoD oversight or investigative activities directed by law or formal committee action.

A5.3.1.3. Other legislative matters requiring SAP access as determined by the Secretary or the Deputy Secretary of Defense or the Secretary of the Air Force

A5.3.2. The term "defense committees" means the Senate Committee on Armed Services, the House of Representatives National Security Committee, and the Defense and National Security Subcommittees of the Committees on Appropriations of the Senate and House of Representatives. For Tactical Intelligence and Related Activities (TIARA) SAPs, the term also includes the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.

A5.3.3. Access to Air Force SAPs will not be granted to any employee of the Legislative Branch serving in the capacity of personal staff to a member of Congress.

A5.3.4. Where possible, the Air Force meets congressional needs for information on SAPs with noncompartmented material. The Air Force gives direct access to compartmented material only when noncompartmented material does not meet congressional need.

A5.3.5. Compartmented access will last only long enough to fulfill the information requirement and only to approved individuals while serving in a capacity requiring such access.

A5.3.6. The Legislative Branch may not keep material DoD protects with compartmented security controls unless the DUSD(P) approves it in advance and the Air Force primary office sponsoring the SAP determines that the retention facilities meet all prescribed security standards for the classification level and any special handling requirements for the materials involved.

A5.3.7. The Department of Defense, DCI, Federal Bureau of Investigation (FBI), Office of Personnel Management (OPM), or other investigative agencies approved by DoD investigate the backgrounds of employees seeking access to compartmented information. The results of the background investigation (BI) must meet the DoD standards for the SAP.

A5.4. SAP Procedures:

A5.4.1. A request for access to Air Force SAP compartmented information must be submitted with the approval of the chair or ranking minority member of a committee or subcommittee with defense oversight. In extremely urgent cases, the Air Force accepts the staff member's signature. The request must include:

A5.4.1.1. Name of individual requiring access.

A5.4.1.2. Social Security number.

A5.4.1.3. Date of most recent BI and name of investigating agency.

A5.4.1.4. Committee or subcommittee capacity in which access is required.

A5.4.1.5. Purpose and duration of required access.

A5.4.1.6. Identification of information required.

A5.4.2. SAP managers process requests for access by:

A5.4.2.1. Submitting them to SAF/AAZ for approval, who coordinates with the responsible OSD office as needed.

A5.4.2.2. Verifying an individual's security clearance before identifying and providing access to compartmented information.

A5.4.2.3. Referring disputes to the DEPSECDEF when Air Force and congressional staff are unable to resolve access issues.

A5.4.3. Promptly notifying SAF/AAZ when individuals granted access no longer require access or are departing the local area so a debriefing can be completed.

Attachment 6

SPECIAL ACCESS HANDLING PROCEDURES

A6.1. The following handling procedures apply to all SAP materials.

A6.1.1. Materials hand-carried from one office to another will be enclosed within a locked security pouch or briefcase.

A6.1.2. Exposed wrapping/packaging material will not display any classified information, i.e., outer cover sheets/wrapings may have unclassified nicknames but will not have codewords. Outer cover sheets/wrappings will have special handling instructions, such as

SPECIAL HANDLING OF THIS DOCUMENT IS REQUIRED. HAND

CARRY DURING ROUTING. NORMAL DISTRIBUTION CHANNELS

WILL NOT BE USED. ACCESS TO THIS DOCUMENT MUST BE

LIMITED ONLY TO THOSE WITH A STRICT NEED TO KNOW.

CONTACT THE PROGRAM OFFICE FOR FURTHER INSTRUCTIONS.

A6.1.3. Wrappings and/or cover sheets will have specific program point of contact (POC)/alternate and telephone number for material retrieval. In the event the program POC cannot retrieve SAP or sensitive materials, instructions will be provided to the recipient to contact a specifically cleared individual for pickup.

A6.1.4. Clearances and access for an individual will be verified prior to leaving material with that individual.

A6.1.5. Only in rare or unusual instances will executive officers, military assistants, or office administration personnel be granted access to SAP information, and then only if there is a bonafide need-to-know. Convenience or efficiency are not legitimate need-to-know criteria.

A6.1.6. Materials will be stored only in program approved storage facilities and security containers. Individuals transporting such materials will ensure recipients understand any specific handling and storage requirements.

Attachment 7

PROGRAM GUIDANCE AND SUPPORT THROUGH SAF/AAZ

Administrative Recourse

Air Force Audits

Artifact Disposition

Codewords

Congressional or White House Inquiries

DoD Annual Reports

Electromagnetic Frequency Management & Communications

Facilities

Foreign Acquisitions and Technology Transfer (Foreign Ownership, Control or Influence (FOIC) and Committees on Foreign Investment in the United States (CFIUS) issues)

Fraud, Waste and Abuse, (FWA) Complaints

Freedom of Information Act (FOIA) Requests

Intelligence & Counterintelligence Support

Investigations

Logistics

News Leaks or Unauthorized Disclosures

Nicknames

Personnel

Post Government Employment with SAP Contractors

Security/Surveys

Attachment 8

SAP REPORT FORMAT (BUDGET REPORT)

(CLASSIFICATION)

(DEPARTMENT and/or AGENCY)
(Unclassified Program Nickname and Classified Program Title)
FY 1994-FY 1995 SAP REPORT

- Resource Summary: (President's budget, dollars in thousands)

Appropriation	Line #	Years	FY1995	FY1996	FY1997	FY1998	FY1999	FY2000	FY2001
RDT&E									
Procurement by PE									
O&M									
MILCON									

- Estimated total program cost: RDT&E/Procurement in Constant FY 1990 $
  (exclude manpower and O&M) *
- Program description: (key objectives of program) **
- Program accomplishments: (actual progress toward objectives)
- Basis for budget request: (why funds are needed in FY94)
- Justification: (rationale for continuation of SAP status)
- Major milestones: N/A if not applicable
- Major contractors: N/A if not applicable
- Delivery schedule: N/A if not applicable
- Production facilities: N/A if not applicable

Action Office:
Phone:

(CLASSIFICATION)

Format: 8 1/2" x 11" bond paper; all margins 1/2", except the left edge, which should be 1"; 12 pitch font. Precede all paragraphs with classification markings. Identify all abbreviations on the page on which they occur. Be clear and concise.

*Note 1 For continuing technology base programs, compute total through FY99. Other programs will include all RDTE and Procurement from program initiation through completion of production.

** Comment separately in the report cover letter on any programs with technologies or missions similar to the specific SAP covered in this report.

Note: Do not staple the final inputs. These become masters from which copies are made.

Attachment 9

SAP SUMMARY REPORT INSTRUCTIONS

A9.1. SAP Summary Reports are required for all Air Force Special Access Programs established by the Secretaries of Defense and the Air Force. They are designed to solicit information from all program offices to comply with established DoD and Air Force requirements. The formal report for the annual summary to DEPSECDEF has two sections. Section 1 solicits headquarters program managers to provide general program information; section 2 focuses on carve-out contracts that may require information from the contractor and/or the system program office (SPO). SAF/AAZ will task appropriate offices 60 days before required due dates and include the prescribed format to be used. Submit one consolidated Program Summary to SAF/AAZ. Follow the program security guide to determine the overall classification of each report. While specific format and data requirements will be provided in formal tasking, the following guidelines are provided to assist in preparing the main report.

A9.1.1. Section 1 provides basic security and administrative information about the program. It's important to identify all subprograms and projects within the SAP. If any of them changed names, give the old and new names. Assess the importance of arms control agreements, changes in threat, and actions taken to protect your information. Attach a metric assessing the program's technological or operational advantage against an adversary or threat (AFPD 16-7).

A9.1.2. Section 2 addresses carve-out contracts. Each program with one or more associated carve-out contracts must include **all subcontractor** carve-outs and a complete copy of section 2 for each carve-out contract. A carve-out contract awards a classified contract to an industrial firm but relieves the Defense Investigative Service of security inspection responsibility. This distinction is particularly important since the Secretary must specifically identify to DEPSECDEF and request approval to continue all carve outs in the annual report.

A9.1.2.1. If inspectors do not use a DD Form 696 (*Industrial Inspection Report*), clearly identify the type of inspection format used.

A9.1.2.2. DD Forms 254 (Contract Security Classification Specification) will be made available upon request.