

**BY ORDER OF THE COMMANDER  
AIR FORCE INTELLIGENCE  
SURVEILLANCE AND  
RECONNAISSANCE AGENCY**

**AIR FORCE ISR AGENCY INSTRUCTION 16-702**

**29 JULY 2011**

**Operations Support**



**MANAGEMENT OF SPECIAL ACCESS  
PROGRAMS WITHIN THE AIR FORCE  
INTELLIGENCE, SURVEILLANCE AND  
RECONNAISSANCE AGENCY (AFISRA)**

**COMPLIANCE WITH THIS PUBLICATION IS MANDATORY**

---

**ACCESSIBILITY:** Publications and forms are available on the e-Publishing website at [www.e-Publishing.af.mil](http://www.e-Publishing.af.mil) for downloading or ordering.

**RELEASABILITY:** There are no releasability restrictions on this publication.

---

OPR: AFISRA/ZQSO

Certified by: AFISRA/ZQ  
(Mr. Bruce Hardy)

Pages: 9

---

This publication implements Air Force Policy Directive (AFPD) 16-7, *Special Actions Programs* and AFI 16-701, *Management, Administration and Oversight of AF Special Access Programs*. It establishes responsibilities for oversight of Special Access Programs (SAPs) within the Air Force Intelligence, Surveillance and Reconnaissance (ISR) Agency (AFISRA). This instruction applies to all AFISRA military, government civilian personnel, contractors and consultants when contract performance depends on access to SAPs, Non-DoD US Government Agencies whose personnel, by mutual agreement, require access to SAPs. The AFISRA Primary Subordinate Units (PSUs) are Air Force Technical Applications Center (AFTAC), National Air and Space Intelligence Center (NASIC), 70th ISR Wing (ISRW), 480 ISRW and 361st ISR Group (ISRG). This publication also applies to AFISRA-gained/attached Air National Guard (ANG) and Air Force Reserve Command (AFRC) organizations. 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 Form 847s from the field through the appropriate functional's chain of command. Maintain records created as a result of the prescribed processes identified in this directory in accordance with (IAW) AFMAN 33-363, *Management of Records*, and dispose of them IAW the AF Records Disposition Schedule (RDS) found on the Air Force Portal link at <https://www.my.af.mil/afirms/afirms/afirms/rims.cfm>. This guidance does not supersede any superior authority or supplant specific authorities provided by Air Force policy directives or instructions to the extent they are inconsistent with this instruction.

**1. General.** AFISRA, as the provider of Air Force ISR forces, has significant participation in and contributions to U.S. Government (USG) special access programs. AFISRA provides forces and capabilities to accomplish Planning, Collection, Processing, Analysis, and Dissemination of intelligence from SAP sensors. AFISRA also ensures SAP weapon systems are provided all intelligence required for development, planning and operations. To accomplish these tasks, the AFISRA/CC approves and directs all Agency participation in SAP activities.

**2. Purpose.** The purpose of this instruction is threefold. First, it ensures appropriate individuals are accessed to programs while protecting extremely sensitive information. Second, it allows the commander to prioritize Agency efforts to maximize accomplishment of all assigned missions and requirements. Third, it allows the commander to provide the required oversight of the expenditure of resources from multiple programs while ensuring compliance with different statutory authorities/requirements for uniquely funded ISR operations.

**3. Scope.** This instruction applies to all AFISRA units and organizations. For the purposes of this instruction, SAP refers to any USG program that requires restricted access beyond the standard classification system and the Sensitive Compartmented Information (SCI) system. These include all categories of SAPs (acquisition, operations and support, and intelligence), as well as those programs managed by other DoD or USG entities. Also included are Alternative Compensatory Control Measures (ACCM) systems, AF COAL WARFIGHTER (CW) and Joint Staff Focal Point (FP) programs, and the Integrated Joint Special Technical Operations (IJSTO) Control systems.

**4. Applicability.** This instruction specifically excludes those situations where the Agency has no explicit program responsibilities (e.g., security, resource oversight, operations, etc.). However, this exclusion does not imply that Agency members may participate in sensitive operations without explicit Agency approval, even if those operations are protected in another agency's SAP.

## **5. Responsibilities**

### **5.1. AFISRA Commander (AFISRA/CC) will:**

5.1.1. Ensure establishment of AFISRA guidance and policy for safeguarding of all information relating to SAPs.

5.1.2. Ensure compliance with higher headquarters guidance and policy.

5.1.3. Assign Agency lead for CW, IJSTO, and FP programs to AFISRA/A3. Establish and assign Agency lead for all other SAPs to a Program Coordination Office (PCO).

5.1.4. Designate in writing a primary and alternate Focal Point Program Control Officer (FPPCO) IAW CJCM 3213.02C to support the Joint Staff Focal Point Program.

### **5.2. AFISRA SAP Program Coordination Office (PCO), AFISRA/ZQ, will:**

5.2.1. Report to the AFISRA/CC and serve as AFISRA/CC's primary representative for all SAP-related issues as the AFISRA PCO. *Note:* Specifically excluding the CW, IJSTO, and FP programs.

5.2.2. Maintain cognizance of all Agency SAP activities.

5.2.3. Serve as the Agency's focal point for SAP policy, guidance, and oversight.

5.2.4. Define roles, relationships, functions, and duties of the PCO staff with Agency subordinate activities and agencies in order to ensure mission accomplishment.

5.2.5. Function as a facilitator by bringing Agency SAP activities together when possible for either integrated planning or management purposes. For operational ISR integrated planning issues use AFISRA's Special ISR Operations Cell (SIOC).

5.2.6. Serve as the Agency focal point for coordination with the Agency staff offices (e.g., A2, A3, etc.) and Primary Subordinate Units (PSUs). Serve as the Office of Primary Responsibility (OPR) for SAPs in support of ISR requirements.

5.2.7. Support the SAP governance structure as an advisor to AF/A2Z for SPRG resource allocation and programmatic matters.

5.2.8. Ensure appropriate Agency and PSU staff offices are granted SAP access to develop and field required ISR forces and capabilities.

5.2.9. Appoint a Government SAP Security Officer (GSSO).

5.2.10. Assist PSUs with obtaining resources required to execute SAP activities.

5.3. AFISRA/A3 will:

5.3.1. Manage the Agency's participation and role in Integrated Joint Special Technical Operations and the AF COAL WARFIGHTER program.

5.3.2. Coordinate with the PCO on all SAP related activities outside the IJSTO and CW program, and inform PCO of any SAP issues within IJSTO and CW that require PCO support.

5.3.3. Notify PCO of any requests for SAP support from outside agencies or SAP activities within AFISRA units.

5.3.4. Ensure appropriate PSU offices are granted access to IJSTO and AF CW programs required to execute ISR operations.

5.4. HQ AFISRA Directorates and their subordinate activities will ensure all SAP related actions/functions are coordinated through the PCO.

5.5. The AFISRA GSSO will:

5.5.1. Provide SAP coordination, distributed security support, and oversight for all HQ-level organizations and Agency subordinate activities to ensure required security programs are established and implemented for the management and protection of SAP activities.

5.5.2. Ensure all Agency-level and subordinate organizations working SAP activities are in compliance with applicable policies, directives, regulations, and instructions.

5.5.3. Ensure SAP security compliance inspections are conducted throughout the Agency in accordance with published SAPCO policy. When requested, assist PSU and subordinate GSSOs with security compliance inspections and/or staff assistance visits (SAVs).

5.5.4. Act as the conduit for all SAP security issues and concerns generated within the Agency and refer issues relating to specific SAPs to the respective AFOSI/PJ Program Security Officer (PSO) or supported activity's PSO.

5.6. Agency PSU Commanders will

5.6.1. Appoint, in writing, an Assistant to the Commander for Special Programs (ACSP).

5.6.2. Ensure that all SAP activities are coordinated with the PCO.

5.6.3. Designate a Focal Point Program Control Office (FPPCO) to support Joint Staff Focal Point program activities and submit appointment letters to the Agency FPPCO. Further delegation of FPPCO duties is authorized only with prior coordination through the AFISRA FPPCO.

5.7. The FPPCO will:

5.7.1. Serve as the organization point of contact for FP information.

5.7.2. Maintain internal organization access control lists.

5.8. The ACSP will:

5.8.1. Serve as the liaison/information conduit between the PCO and the respective PSU Commander as well as subordinate unit SAP activities to include geographically separated units (GSU).

5.8.2. Function as the PSU focal point for Agency SAP resources, programmatic, and security taskings/suspenses.

5.8.3. Function as a facilitator by bringing PSU SAP activities together when possible for either integrated planning or management purposes.

5.8.4. Ensure all requests for participation in support of another government-sponsored SAP are made through Agency channels (e.g., ACSP through the PCO, to the AF/A2 SAPMO, to the AF SAPCO).

5.8.5. Notify the PCO of any SAP-related activities not specifically delegated and coordinated through the Agency as part of the individual organization's designated mission support activities or as outlined in an AF SAPCO approved Memorandum of Agreement.

5.8.6. Submit SAP resource requirements to the AFISRA SAP PCO or other cleared HQ staff office as appropriate. Contact the PCO for specific guidance, if required.

5.8.7. Ensure sufficient personnel are granted access to SAP programs to sufficiently execute tasked ISR development, fielding and execution activities.

5.8.8. Appoint a PSU GSSO.

5.9. The PSU GSSO will:

5.9.1. Function as the SAP security lead for the PSU.

5.9.2. Provide SAP security management, oversight and compliance verification of all SAP activities within their PSU, to include the PSU's GSUs.

5.9.3. Ensure all SAP activities conduct annual security self-inspections in accordance with applicable policies and directives.

5.9.4. Ensure all documentation related to co-utilization agreements (CUAs) and Memorandums of Agreement (MOAs)/Memorandums of Understanding (MOUs) established to support a SAP activity are sent through the PCO for coordination with the SAPMO. **Note:** The PCO will be coordinated with on all CUAs, MOAs and MOUs prior to entering into a support arrangement and before forwarding to the SAPCO.

5.9.5. Ensure all SAP material is properly stored, secured, and safeguarded.

**6. Reporting Requirements.** ACSP/PSU GSSOs will report the following information to the PCO no later than 31 January each year:

6.1. Number of facilities used to support SAP activities. Provide a complete list of the PSU's separately accredited facilities [Special Access Program Facility (SAPFs), Sensitive Compartmented Information Facility (SCIFs) and Temporary Secure Working Areas (TSWA) approved to store, discuss and process SAP information].

6.2. Number of information systems processing SAP data (e.g., networks, LANs, WANs, stand alone, laptops, etc.).

6.3. Number of personnel accessed to SAPs by unit/organization (e.g., 480 ISRW (250), 361 ISRG (25), NASIC (220), etc.).

6.4. Number of Top Secret SAP documents and media (e.g., hard drives, DVDs, CDs, data tapes, flash drives, etc.).

6.5. Date and scope of last SAP Security Compliance Inspection (e.g., Core Compliance Items (CCI), Full Scope, Staff Assistance Visit (SAV), or Follow-up).

6.6. Date of last 100 percent inventory of Top Secret SAP material (documents and media).

6.7. Number of Co-Use Agreements (CUAs), Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) to include the date of the agreements.

6.8. Updated list of primary Program Security Officer (PSO) for supported SAP activities (e.g., AFSPC PSO, John Doe; DOJ PSO, Jane Doe; CIA PSO, Santa Claus, etc.).

6.9. All suspected instances of SAP information being compromised to the PCO and respective AFOSI/PJ PSO or supported activity equivalent within 24 hours of discovery of such instance in accordance with applicable directives and/or regulations.

6.10. Any incident/situation that could negatively affect SAPs and cause senior leader attention to the PCO, who will in turn notify AFISRA/CC.

**7. Security Inspections.**

7.1. Self-Inspections.

7.1.1. All Agency SAP activities operating within a special access program facility (SAPF) will conduct a documented annual self-inspection using the most current inspection checklist.

7.1.2. Self-inspections will be thorough and complete. Address each item on the checklist with a comment to illustrate how the requirement is met. Provide explanations

for requirements not met or not applicable. Use the AFISRA Security Compliance Self-Inspection Handbook as a reference for conducting self-inspections.

7.1.3. ACSPs will review and submit unit SAP security self-inspection report to the cognizant PSO within 30 days of completion.

7.2. Security Compliance Inspections. The PCO and GSSOs in coordination with cognizance Security Inspection authorities will ensure Agency SAP activities are scheduled for security compliance inspections every 12 to 24 months as determined by the appropriate inspection entity.

**8. Memorandums of Agreement (MOA)/Memorandums of Understanding (MOU).** MOA/MOUs between Agency organizations and non-AF organizations will be approved by the SAPCO. Within AFISRA, these MOA/MOUs will be staffed through the PCO for SAPMO coordination and SAPCO approval.

**9. Freedom of Information Act (FOIA) Requests.** All FOIA requests regarding SAP information will be processed by the SAPCO. Upon receipt of FOIA request, the organization will request the local FOIA office transfer the request to SAF/AAZ.

BRADLEY A. HEITHOLD, Maj Gen, USAF  
Commander

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

AFPD 16-7, *Special Actions Programs*, 29 December 2010

AFI 16-701, *Management, Administration and Oversight of AF Special Access Programs*, 1 November 2005

AFI 31-401, *Information Security Program Management*, 1 November 2005

AFI 31-501, *Personnel Security Program*, 27 January 2005

AFI 31-601, *Industrial Security Program*, 29 June 2005

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

AFPD 90-2, *Inspector General – The Inspection System*, 26 April 2006

AFI 90-201, *Inspector General Activities*, 17 June 2009

DCID 6/3, *Protecting Sensitive Compartmented Information within Information Systems (DCID 6/3)-Manual*, 5 June 1999

ICD 704, *Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Controlled Access Program Information*, 1 October 2008

ICD 705, *Sensitive Compartmented Information Facilities*, 26 May 2010

DoDD 5200.1-R, *Information Security Program and Regulation*, 14 January 1997

DoDD 5205.7, *Special Access Program (SAP) Policy*, 1 July 2010

DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, 28 February 2006

JAFAN 6/0, *Special Access Program Security Manual*, 29 May 2008

JAFAN 6/3, *Protecting Special Access Program Information within Information Systems*, 15 October 2004

JAFAN 6/4, *Special Access Program Tier Review Process*, 9 May 2006 (Revision 1)

JAFAN 6/9, *Physical Security Standards for Special Access Program Facilities*, 23 March 2004 (Change 1, 20 December 2005)

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication*

***Abbreviations and Acronyms***

**ACSP**—Assistant to the Commander for Special Programs

**AF**—Air Force

**AFADS**—Air Force Access Database System

**AFISRA**—Air Force Intelligence, Surveillance and Reconnaissance Agency

**AFOSI**—Air Force Office of Special Investigation

**AFRC**—Air Force Reserve Command

**AFTAC**—Air Force Technical Applications Center

**ANG**—Air National Guard

**CAP**—Corrective Action Plan

**CC**—Commander

**COMPSO**—Command Program Security Officer

**CUA**—Co-Use Agreement

**CW**—Coal Warfighter

**DCID**—Director of Central Intelligence Directive

**DoD**—Department of Defense

**DT&E**—Developmental Test and Evaluation

**ECD**—Expected Completion Date

**FOIA**—Freedom of Information of Act

**FP**—Focal Point

**FPPCO**—Focal Point Program Control Officer

**GSSO**—Government SAP Security Officer

**GSU**—Geographically Separated Unit

**JAFAN**—Joint Air Force, Army and Navy

**MOA**—Memorandum of Agreement

**MOU**—Memorandum of Understanding

**IAW**—In Accordance With

**IJSTO**—Integrated Joint Special Technical Operations

**ICD**—Intelligence Community Directive

**ISRG**—Intelligence, Surveillance and Reconnaissance Group

**ISRW**—Intelligence, Surveillance and Reconnaissance Wing

**NASIC**—National Air and Space Intelligence Center

**OPR**—Office of Primary Responsibility

**PCO**—Program Coordination Office

**PSO**—Program Security Officer

**PSU**—Primary Subordinate Units

**RDS**—Records Disposition Schedule

**SAPCO**—Special Access Program Central Office (SAF/AAZ)

**SAP**—Special Access Program

**SAPF**—Special Access Program Facility

**SAPMO**—Special Access Program Management Office (HAF/A2Z)

**SAV**—Staff Assistance Visit

**SCIF**—Sensitive Compartmented Information Facility

**SPRG**—Special Program Review Group

**SSG**—SAP Steering Group

**TSWA**—Temporary Secure Working Area

**USG**—U.S. Government