

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



**AIR FORCE INSTRUCTION 16-701**

**18 FEBRUARY 2014**

**AIR FORCE OPERATIONAL TEST AND  
EVALUATION CENTER  
Supplement**

**15 OCTOBER 2015**

**Operations Support**

**MANAGEMENT, ADMINISTRATION  
AND OVERSIGHT OF 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](http://www.e-Publishing.af.mil) for downloading or ordering

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

---

OPR: SAF/AAZE

Certified by: SAF/AAZ  
(Mr. Daniel F. McMillin)

Supersedes: AFI 16-701, 1 November  
1995 and AFI 16-702, 1 September 1998

Pages: 53

**(AFOTEC)**

OPR: AFOTEC/A-3Z

Certified by: AFOTEC/A-3  
(Mr. Grant Schaber)

Supersedes: AFI16-701\_AFOTECSUP,  
17 February 2011

Pages: 6

---

This Air Force Instruction (AFI) implements DoD Instruction (DoDI) 5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, and AF Policy Directive (AFPD) 16-7, *Special Access Programs*. It establishes responsibilities for the management, administration and oversight of SAPs for which the Air Force has cognizant authority (CA), hereafter referred to as SAPs. This instruction applies to all military, government civilian personnel, contractors and consultants when contract performance depends on access to these 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 should require the non-DoD party's compliance with this guidance. 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 AFI may be supplemented at any level, but all supplements must be routed to the Secretary of the Air Force, Security, Counterintelligence, and Special Program Oversight (SAF/AAZ) for coordination, prior to certification and approval. 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/afirms/afirms/afirms/rims.cfm>. This guidance does not supersede any superior authority or supplant specific authorities provided for by Air Force policy directives or instructions, to the extent they are inconsistent with this instruction. The disclosure provisions in this instruction 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 instruction and are controlling.

**(AFOTEC)** This publication implements DoD Instruction (DoDI) 5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs), and AF Policy Directive (AFPD) 16-7, Special Access Programs. It establishes responsibilities for the management, administration and oversight of SAPs for which the Air Force has cognizant authority. This supplement identifies roles and responsibilities to effectively manage Special Access Programs within AFOTEC and is applicable to all AFOTEC Detachments, Directorates, Operating Locations and special staff including the Command Section. This publication may not be supplemented.

**(AFOTEC)** AFI 16-701, 18 February 2014, is supplemented as follows:

### ***SUMMARY OF CHANGES***

This document has been substantially revised and must be completely reviewed. It incorporates the appeal board requirements for special access programs previously documented in AFI 16-702.

1.	Guidance.....	3
2.	Roles and Responsibilities.....	6
3.	SAP Governance.....	23
4.	SAP Management, Administration and Oversight.....	23
Figure 1.	Notional SAP Security Architecture.....	25
Table 1.	Establishment Request Required Elements.....	25

Table 2.	Information required for Request for SAP Inclusion in War-games or Exercises..	28
Table 3.	Program Protection Elements .....	29
Table 4.	IJSTO Apportionment Package Requirements .....	31
Table 5.	Disestablishment Plan Elements .....	32
	5. Support to Non-AF SAPs. ....	33
Table 6.	Items Required in MOA For SAPs Directed By Another DoD Component or Agency .....	33
Table 7.	MOA Elements Required for a SAP System Capability Transfer .....	34
	6. The Appeal Board For SAP Access.....	34
	7. Foreign Ownership, Control or Influence (FOCI). ....	36
<b>Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION</b>		<b>39</b>
<b>Attachment 2— INSTRUCTIONS FOR APPEAL BOARD APPEARANCES (REQUEST FORMAT EXAMPLE)</b>		<b>48</b>
<b>Attachment 3— INSTRUCTIONS FOR APPEAL BOARD APPEARANCES (RESPONSE FORMAT EXAMPLE)</b>		<b>49</b>
<b>Attachment 4— SAMPLE – NATIONAL INTEREST DETERMINATION (NID) REQUEST PACKAGE</b>		<b>50</b>

## 1. Guidance.

1.1. All SAPs shall be assigned an unclassified nickname to facilitate program protection and administration and Congressional reporting requirements. The Director, AF Special Access Program Central Office (SAPCO), shall determine whether a classified code word shall also be used. Unclassified nicknames shall be used in the SAP annual report to Congress. SAP security classification guides (SCGs) shall be consulted for guidance on handling nicknames and code words as they may be handled via SAP channels only.

1.2. The Defense Security Service (DSS) has National Industrial Security Program (NISP) security oversight responsibility for all SAPs unless specifically requested by the Secretary of the Air Force (SECAF) to be carved-out by the Secretary of Defense (SecDef) or Deputy Secretary of Defense (DepSecDef). When the carve-out is approved, the Air Force assumes the NISP security oversight responsibility and is executed by Air Force Office of Special Investigation (AFOSI) PJ with SAF/AAZ oversight. Regardless of the carve-out status of the SAP, DSS is responsible for issuing facility security clearances (FCL) for all defense contractors performing work for all SAP contracts. With both DSS and government contracting activities (GCAs) involved with industrial security responsibilities, total oversight of a cleared defense contractor is contingent upon DSS's ability to confirm carve-

out contract arrangements or areas. DSS must be able to refer security issues or notify GCAs exercising SAP security oversight on issues affecting the overall security posture of a defense contractor.

1.3. An SCG outlining the critical program information (CPI) shall be developed for each SAP, compartment, sub-compartment and project. SCGs shall be approved by a SAP original classification authority (OCA) as appointed by the SECAF. All SAP SCGs must be endorsed by the Security Director, AFOSI PJ. SCGs shall be reviewed, updated, and reissued as circumstances require, but at least once every five years. OCAs shall issue declassification instructions to facilitate effective review and declassification of information classified under predecessor executive orders. These instructions may be in the form of separate guides, sections of classification guides, memoranda, etc. Copies of all SCGs and classification guidance shall be provided to the Director, AF SAPCO, who shall maintain a copy and make available to the Director, DoD SAPCO. Copies of SCGs may be obtained through a program security officer (PSO).

1.4. Prior to gaining access and during the period of access to SAPs, all personnel shall consent to, and be subject to, a random counterintelligence (CI)-scope polygraph examination. All personnel must sign a SAP indoctrination agreement documenting this consent. Polygraph examinations are considered current when administered within the past five years. CI-scope polygraph examinations shall not be used as the only basis for granting access to SAPs. Polygraph examinations are authorized for use as a part of a risk mitigation strategy to resolve security or CI issues regarding SAP accessed individuals. Polygraph examination results will be maintained IAW DoDI 5210.91. Air Force policy and processes preclude AF personnel from undergoing life style polygraph examinations. Any requests by other government agencies to administer a life style polygraph examinations shall be forwarded to the Director, AF SAPCO, for resolution.

1.5. The Air Force Access Database System (AFADS), or any successor, shall be the Air Force's single, authoritative SAP system containing individual SAP access information for all personnel accessed to SAPs. When warranted, the Director, AF SAPCO, may exempt select SAPs from inclusion in AFADS. When exempted from AFADS, the SAP shall be maintained in the Distributed Common Access Database System (DCADS). Office of Secretary of Defense (OSD) personnel shall be entered into DCADS as the primary authoritative access record and may also be entered into AFADS when necessary for visit certifications to an AF unit and AF IS adjudication.

1.6. The Configuration and Security Tracking System (CASTS), or its successor, shall be the Air Force's single, authoritative, SAP system used to identify all SAP facilities (SAPFs) and those that are joint with other DoD SAPFs or sensitive compartmented information (SCI) facilities (SCIFs). The AF SAPCO shall approve all exceptions.

1.7. All SAPs shall include current arms control and treaty compliance requirements, obligations, and constraints as an integral part of the policy, planning, operations and acquisition process. SAPs resident on a military installation shall be included in the installation treaty support plan. For unacknowledged SAPs, or any SAP designated by the PSO, a separate SAP annex to the installation treaty support plan may be required by the PSO. All associated government and contractor facilities that have SAP activities shall have site-specific treaty inspection plans that include detailed managed access provisions. SAP

activity treaty inspection readiness plans must be approved by the PSO and are subject to annual review and certification.

1.8. All requests for Congressional Members or staffs to gain access to SAP information must be forwarded to the Special Programs Oversight Committee (SPOC) Executive Secretary. All personnel engaging Congress, to include visits with members and staff, to discuss SAPs shall obtain the approval of the DoD SAPCO through the SPOC Executive Secretary prior to briefing or providing SAP information. The SPOC Executive Secretary shall inform the Director, AF SAPCO, when noncompliance or issues arise related to Congressional interaction. The Director, AF SAPCO, shall review all reported noncompliance.

1.9. Access to a SAP shall be strictly limited to the minimum number of personnel necessary for execution of the program. Granting access to a SAP shall be based solely upon a determination that the individual has a valid need-to-know (NTK), has the requisite security clearance, meets approved personnel prerequisites, and shall clearly and materially contribute to the execution or oversight of the SAP. Access is never authorized for convenience alone nor mandated singularly by position or rank. Accordingly, executive officers and military assistants shall not be routinely accessed to SAPs. Individuals assigned to these positions must have a valid NTK and demonstrate how they shall materially contribute to the SAP before access shall be granted. In addition, the DepSecDef's statutory authority to approve all waived program access for Office of the Secretary of Defense (OSD) personnel and for all government employees external to the Department of Defense shall not be delegated. Access to SAPs, categorized as waived, require additional scrutiny by the Access Approval Authority (AAA) (e.g., mandatory billet plans).

1.10. All DoD government and contractor personnel accessed to SAPs are required to bring all available information regarding any scheduled or proposed legal proceeding that involves the potential disclosure, use or discussion of SAP material, to the attention of the PSO. The PSO shall report to the Security Director, AFOSI PJ, within 48 hours of learning thereof. The Security Director, AFOSI PJ, shall report to the Director, AF SAPCO, as soon as possible.

1.11. The Air Force shall protect SAPs at all times consistent with their classification and sensitivity.

1.12. The Air Force shall ensure appropriate review and compliance with Intelligence Oversight requirements for all SAPs.

1.13. The Air Force shall ensure compliance with the Management Internal Control Program. All critical program information will be protected in accordance with the program SCG.

1.14. All government and contractor organizations that create, handle, or store SAP information must appoint an official to serve as SAP security officer [e.g., government SAP security officer (GSSO), contractor program security officer (CPSO), information system security manager (ISSM), information system security officer (ISSO)] for the activity, to properly manage and oversee the activity's SAP security activities.

1.15. SAP-accessed personnel will coordinate with their SAP security officer, who will contact the PSO, for all recommendations for technologies or capabilities that may require SAP protections.

1.16. Privileged users shall be accessed to all SAPs on the ISs in which they have privileged access.

1.17. Required SAP management, administration, and oversight procedures are provided in Section 4.

## **2. Roles and Responsibilities.**

2.1. The Director, Security and Special Program Oversight (SAF/AAZ), shall:

2.1.1. Serve as the principal advisor to SAF/AA for SAPs.

2.1.2. Serve as the Director, AF SAPCO, and develop SAP policies and procedures for management, administration and oversight of SAPs. In addition, the AF SAPCO is responsible for directing, administering, and overseeing the SAP security program.

2.1.2.1. Ensure adequate resources for a robust SAP security program are identified.

2.1.2.2. Provide oversight for a SAP security education, training and awareness (SETA) program.

2.1.2.3. Serve as the SAP functional security manager for SAP security policy, define SAP security inspection criteria and evaluate government and contractor SAP security compliance inspection trends for potential changes in policy, training, SAP security inspection criteria, etc.

2.1.2.4. Establish a declassification program and ensure that necessary resources are applied to the review of information to ensure it is neither classified for longer than necessary nor declassified prematurely in accordance with the file series exemption.

2.1.2.5. Define security policy and guidance on the use of SCI in association with the execution of SAPs, in coordination with AF/A2.

2.1.2.6. Serve as the Designated Accreditation Authority (DAA) for all SAP ISs. DAA for ISs may be delegated, in writing, and shall be revalidated annually. This DAA delegation may not be further delegated unless approved by the Director, AF SAPCO.

2.1.2.7. Serve as the AAA for all SAPs and approve waivers for SAP access. When the Director delegates AAA, it shall be in writing and annually revalidated. All AAA delegations shall be coordinated with respective OCAs. This AAA delegation may not be further delegated unless approved by the Director.

2.1.2.8. Evaluate the annual (due by January 31) security and investigation trend analysis report on industry from the Security Director, AFOSI PJ, and identify potential changes to SAP security policy.

2.1.2.9. Act as the focal point between the Air Force and the DSS to ensure SAP security education and training curriculum requirements are integrated into the DSS training portfolio for security professional certification. The Director shall support the DoD Security Professional Education Development (SPeD) program and ensure Office of Personnel Management certifications are integrated into the SAP security training program.

- 2.1.2.10. Within SAP security constraints, ensure the performance contract or other system used to rate the performance of civilian and military personnel includes the designation and management of SAP information as a critical element or item to be evaluated in the rating of (1) SAP original classification authorities, (2) SAP security officers, (3) personnel who derivatively classify SAP information on a routine basis, (4) SAP information systems security personnel if their duties involve access to SAP information and information system personnel with privileged access to SAP systems or network resources, and (5) all other personnel whose duties include significant involvement with the creation or handling of SAP information.
- 2.1.2.11. Establish procedures for receipt of information, allegations, or complaints regarding over classification or incorrect classification, as needed, and provide guidance to personnel on proper classification for SAPs.
- 2.1.2.12. Submit to the Director of Security, Office of Under Secretary of Defense for Intelligence (OUSDI), an annual report listing, by position title, those officials within the Air Force who hold SAP original classification and declassification authority.
- 2.1.2.13. Appoint the Chair to the SAP Personnel Security Appeal Board (PSAB).
- 2.1.2.14. Provide oversight of the NISP for SAPs. Support PSOs, in cooperation with the Head GCA, in evaluating contractors against security criteria when a carve-out contract exists.
- 2.1.2.15. Validate annually green door positions supporting SAPs in coordination with AIM.
- 2.1.3. Be responsible to support the DoD SAPCO and shall:
- 2.1.3.1. Immediately inform the DoD SAPCO of any significant issue of a security nature and of SAP personnel access suspensions, revocations and reinstatements.
- 2.1.3.2. Submit all Prospective SAP (PSAP) requests to the Director, DoD SAPCO for SecDef approval.
- 2.1.3.3. Provide to the Director, DoD SAPCO, all requests to take the following actions:
- 2.1.3.3.1. Disestablish SAPs.
- 2.1.3.3.2. Changes to SAP scope, types, categories, and security classifications.
- 2.1.3.3.3. Changes to oversight authority (OA) or CA.
- 2.1.3.3.4. Transition from special access enhanced security controls.
- 2.1.3.3.5. Apportionment and de-apportionment of SAPs into and out of the Integrated Joint Special Technical Operations (IJSTO).
- 2.1.3.3.6. Use of AF resources to support non-AF SAPs, when approved by SECAF.
- 2.1.3.3.7. Include foreign participation or share information about SAPs with foreign entities.

- 2.1.3.3.8. Relieve (carve out) the DSS of their security oversight role.
  - 2.1.3.4. Review all memorandums of agreement (MOA) and memorandums of understanding (MOU) that have any international involvement with SAPs. The Director shall review and make recommendations about the international security portions of SAPs and related program information and capabilities to the DoD SAPCO for SecDef approval.
  - 2.1.3.5. Provide the SECAF the Air Force submission to the SAP annual report for final signature and submit to the DoD SAPCO for submission to Congress.
  - 2.1.3.6. Approve the establishment or disestablishment of all compartments, sub-compartments and projects and register nicknames and code words with the Code Word, Nickname, and Exercise Term (NICKA) database. Ensure program identifiers, (PIDs), nicknames, and code words are de-conflicted with DCADS or its successor and forward to the Director, DoD SAPCO.
  - 2.1.3.7. Coordinate on all SAP disestablishment plans.
  - 2.1.3.8. Provide information, as defined by the Director, DoD SAPCO, to meet reporting requirements for carve-outs and treaty compliance.
  - 2.1.3.9. Submit a consolidated report annually through the Director, DoD SAPCO, to the Information Security Oversight Office, National Archives and Records Administration that captures actions taken in support of the SAP file series exemption and records declassification.
  - 2.1.3.10. In coordination with SAF/GCI, review all proposed test packages that require OSD approval.
  - 2.1.3.11. Serve as the central AF focal point with Joint Staff for coordination of Joint Capabilities Integration Development System (JCIDS) activities. The Director shall also approve SAP accesses for Air Force and non-Air Force representatives to the (JCIDS) process for those SAPs that the Air Force has CA.
  - 2.1.3.12. Coordinate with DoD SAPCO to determine which DoD SAP accesses are required for the Air Force representatives to the SAP Oversight Committee (SAPOC), 3-Star Programmer's Review, and SAP Deputy's Management Action Group (DMAG).
  - 2.1.3.13. Ensure AF representatives to the SAPOC are prepared on SAP issues.
  - 2.1.3.14. Support SAF/AQL to resolve issues of security, foreign technology transfer and export issues related to SAPs.
  - 2.1.3.15. Review all reported noncompliance of the Air Force Congressional interaction policy for potential revocation of SAP access.
  - 2.1.3.16. Notify SAF/AA of any SAP that requires involvement of cover, cover support, or cover tradecraft.
- 2.1.4. In addition, the AF SAPCO is also responsible to:
- 2.1.4.1. Chair the SAP Oversight Review Board (SORB).

- 2.1.4.2. Approve National Interest Determinations (NIDs) for all SAPs.
  - 2.1.4.3. Approve all requests for changes to the COAL WARFIGHER (CW) access management plan (AMP) after coordination with all OCAs with equities and AF/A3/5.
  - 2.1.4.4. Review SAP IJSTO apportionment requests and notify SECAF prior to AF/A3/5 approval.
  - 2.1.4.5. Review all SAP public affairs releases (i.e., news releases and all public disclosures), prior to the SECAF's approval.
  - 2.1.4.6. Approve SAPs, in coordination with OCA(s), for inclusion in Quadrennial Defense Reviews (QDR), Scientific Advisory Board (SAB) studies and other special studies, as required.
  - 2.1.4.7. Establish a SAP records management program to ensure SAP records are maintained IAW AFPD 33-3.
  - 2.1.4.8. Support PSOs, in cooperation with the head GCA, in evaluating contractors against security criteria when a carve out contract exists.
  - 2.1.4.9. Ensure SAF/AQL, SAF/GCI, SAF/FMBIB, SAF/AQCS, AF/A8PE and AFOSI PJ, at a minimum, are briefed to the non-AF SAP(s) in order to provide SECAF approved appropriate Air Force support. Additionally, for DoD SAPCO situational awareness, AF SAPCO will inform DoD SAPCO of all new proposals from non-AF entities to support non-AF SAPs.
  - 2.1.4.10. Notify DoD SAPCO of all Committee on Foreign Investments in the United States (CFIUS) issues.
  - 2.1.4.11. Coordinate with SAF/CIO A6 and DoD CIO to:
    - 2.1.4.12. Ensure SAP accesses for SAF/CIO A6 to meet AF CIO requirements (i.e., Clinger-Cohen Act certification).
    - 2.1.4.13. Ensure that SAP ISs and IT comply with statutory, DoD and AF policies.
    - 2.1.4.14. Oversee the implementation of sound and integrated ISs enterprise architecture and standards for SAPs.
    - 2.1.4.15. Promote the effective and efficient design and operation of all major information management processes for the SAPs.
    - 2.1.4.16. Ensure IT/IA governance and compliance across the SAP enterprise.
- 2.2. The Division Chief, Special Programs Division (AFAA/AGS), shall:
- 2.2.1. Serve as the principal advisor to SAF/AG for SAPs.
  - 2.2.2. Serve as the primary focal point for all SAP audit activities.
  - 2.2.3. Perform financial and operational audits on all SAPs and maintain an audit system to record these audits.
- 2.3. The Director, Contracting - Special Programs (SAF/AQCS), shall:

2.3.1. Serve as the senior contracting advisor to the Deputy Assistant Secretary (DAS) (Contracting), SAF/AQC (DASC) for SAPs.

2.3.2. Provide direction and guidance for all matters relating to contract policy for all SAPs.

2.3.3. Ensure SAP contracting offices assist PSOs in evaluating contractors against security criteria when a carve out contract exists.

2.3.4. Ensure the appropriate MAJCOM/PK or Director of Contracting for field offices is aware of contracting support to SAPs within their command or office responsibility, and coordinates on support agreements. In conjunction with SAF/AQL, assigns non-Air Force SAPs to MAJCOMS, direct reporting units (DRUs) and field operating agencies (FOAs) for execution.

2.3.5. Ensure all SAP GCAs submit all NID applications to SAF/AAZ.

2.4. The Director, Special Programs (SAF/AQL), shall:

2.4.1. Serve as the principal acquisition advisor to the Assistant Secretary of the Air Force, Acquisition (SAF/AQ) for SAPs.

2.4.1.1. Provide oversight of acquisition policy, management and execution for SAPs.

2.4.1.2. Serve as the Office of Research and Technology Applications (ORTA) for SAPs and approve all SAP domestic technology transfers (including both internal and external to the Air Force).

2.4.1.3. Assess all acquisition policy and instructions for application to SAPs and establish acquisition policy specific to SAPs.

2.4.1.4. Provide acquisition technical support for developing advanced air, space and cyber systems and subsystems across all phases of the acquisition life-cycle.

2.4.1.5. Provide SAP milestone guidance and support.

2.4.1.6. Review and coordinate on SAP system requirements defined by MAJCOMS, DRUs, and FOAs.

2.4.1.7. Recommend SAP capabilities for inclusion in and removal out of the IJSTO system.

2.4.1.8. Ensure that acquisition community structures, policies, and processes are in compliance with statutory and regulatory requirements for acquisition oversight, economic efficiency, innovative contracting methods, earned value management, information assurance, and interoperability and supportability (including intelligence supportability) requirements.

2.4.1.9. Review CFIUS applications for SAP equities and provide recommendations to SAF/AAZ for incorporation into the OSD response.

2.4.1.10. Resolve issues of foreign technology transfer and export requests related to SAPs. Notify the Directors of the AF and DoD SAPCO when issues arise for SecDef approval.

- 2.4.1.11. Represent the AF as a member of the Low Observable/Counter-Low Observable Tri-Service Committee and Defensive Systems Committee.
  - 2.4.1.12. Coordinate Air Staff level SAP contracting documents (e.g., justification and authorizations, determinations and findings, acquisition strategies, acquisition plans, contracts) through the Director, SAF/AQCS. In conjunction with SAF/AQCS, assign non-Air Force SAPs to MAJCOMs, DRUs, and FOAs for execution.
  - 2.4.1.13. Support PSOs, in cooperation with the head GCA, in evaluating contractors against security criteria when a carve out contract exists, in cooperation with the Director, AF SAPCO.
  - 2.4.1.14. Coordinate and facilitate requests for SAP patents with SAF/GCQ.
- 2.4.2. Serve as the principal advisor to the SECAF, USECAF, and CSAF for SAPs (except for Program Objective Memorandum (POM) matters which are shared with AF/A8P) and as the SPOC Executive Secretary and shall:
- 2.4.2.1. Notify SAF/AAZ, SAF/LLW and SAF/FMB, as required, of all Congressional SAP engagement and obtain the approval of the Director, DoD SAPCO prior to the release of SAP information. In addition, the SPOC Executive Secretary shall notify the Director, AF SAPCO, for all issues (including noncompliance with this policy) associated with congressional interaction.
  - 2.4.2.2. Ensure AF representatives to the SAPOC are prepared on SAP issues.
  - 2.4.2.3. Ensure AF representatives to the 3-Star Programmer's Review and SAP DMAG are prepared on SAP issues in conjunction with AF/A8PE.
  - 2.4.2.4. Recommend SAPs for AF SAPCO approval, in coordination with OCA(s), for inclusion in QDRs, SAB studies and other special studies, as required. Upon approval, provide subject matter expert (SME) support to the execution of these activities.
  - 2.4.2.5. Coordinate SAP resource allocation and programmatic matters with DoD SAPCO. In addition, coordinate programmatic SAP matters with the Joint Staff, OSD (in coordination with AF/A8PE), COCOMs, Congress and other government agencies, as required.
  - 2.4.2.6. Prepare and present the annual OSD Program and Budget Review (PBR) submissions to the Director, Cost Assessment and Program Evaluation (DCAPE) and OUSD Comptroller with SAF/FMBIB and AF/A8PE.
  - 2.4.2.7. Prepare and present the OSD mid-year review submissions to OUSD Comptroller with SAF/FMBIB and AF/A8PE.
  - 2.4.2.8. Coordinate with AF/A8PE for day-to-day integration and de-confliction with the Air Force Corporate structure.
  - 2.4.2.9. Participate in periodic reviews of program funding performance and execution (including intermediate budget reviews), conduct reviews of all financial documentation, and provide day-to-day financial execution and oversight with SAF/FMBIB.

- 2.4.2.10. Present information to various requirements and acquisition bodies, to include the Defense Acquisition Board (DAB), Joint Requirements Oversight Council (JROC), and OSD's Acquisition Overarching IPTs.
  - 2.4.2.11. Maintain liaison with other military services, OSD, defense agencies, and other federal departments to ensure cross-utilization of advanced technologies, where appropriate.
  - 2.4.2.12. Ensure all SAPs have a SAP Directive (SAPD).
  - 2.4.2.13. Coordinate with SAF/AAZ on MOAs and MOUs for SAPs when AF SAP resources are involved for which the SPOC Executive Secretary has been given oversight authority.
  - 2.4.2.14. Coordinates requests for non-AF SAP support in cooperation with SAF/AAZ.
- 2.5. The Director, Special Programs – Budget Investment (SAF/FMBIB), shall:
- 2.5.1. Serve as the principal advisor to SAF/FM for AF SAPs and non-AF SAPs.
  - 2.5.2. Serve as the focal point for SAP financial management policy and oversight.
  - 2.5.3. Oversee the financial structure, budget, cost, accounting controls, execution, and comptroller functions including audit liaison for SAPs.
  - 2.5.4. Execute Management Internal Control Program oversight, including program reviews, site visits, on-site training, and other activities for all SAPs.
  - 2.5.5. Approve financial management and accounting activities for all SAPs.
  - 2.5.6. Participate in periodic reviews of program funding performance and execution (including intermediate budget reviews), conduct reviews of all financial documentation, and provide day-to-day financial execution and oversight in conjunction with SAF/AQL.
  - 2.5.7. Act as the primary interface with the OSD comptroller and support meetings with congressional appropriation committees in coordination with the SPOC Executive Secretary.
  - 2.5.8. Prepare and present annual OSD PBR submissions with the SAF/AQL and AF/A8PE.
- 2.6. The Deputy General Counsel, Intelligence, International, & Military Affairs (SAF/GCI) shall:
- 2.6.1. Serve as the principal advisor to SAF/GC for SAPs.
  - 2.6.2. Serve as the primary focal point for all SAP legal requirements.
  - 2.6.3. Coordinate the participation of other SAF/GC offices, as required, for specialized legal review support. This includes PSAP legal reviews, legal reviews of new SAP capabilities prior to entry into the IJSTO system, Economy Act determinations in support of non-AF SAPs, SAP patents, SAP reports, and legal reviews for testing, training, etc., when required.
  - 2.6.4. Oversee legal review process for all SAPs.

2.6.5. Review, as part of SAP annual reporting and revalidation, the SAP annual report for compliance with applicable laws, executive orders, regulations, and DoD policies.

2.7. The Director, Inspections Directorate (SAF/IGI), shall:

2.7.1. Serve as the principal advisor for inspections to The Inspector General (TIG) and the Deputy Inspector General (DIG) for SAPs.

2.7.2. Implement a SAP fraud, waste, abuse and corruption program.

2.7.3. Conduct government compliance inspections of SAPs IAW DoD guidance and AF policies and report results as directed by the SECAF or CSAF and notify the AF SAPCO of SAP security compliance inspection trends for potential SAP security policy updates or updates to the SAP security inspection criteria.

2.8. The Division Chief, Weapons Systems Liaison Division (SAF/LLW), shall:

2.8.1. Serve as the principal advisor to SAF/LL for SAPs.

2.8.2. Assist the SPOC Executive Secretary with Congressional interaction, as requested.

2.9.

2.10. The Director, Special Programs (AF/A2Z), shall:

2.10.1. Serve as the principal advisor to the AF/A2 for SAPs and as AF/A2's operational lead to organize, train, and equip AF intelligence, reconnaissance, and surveillance (ISR) elements to support joint force SAP capabilities.

2.10.2. Advocate for ISR requirements for SAPs within AF/A2 mission areas.

2.10.3. Provide Intelligence Requirements certification recommendation for SAPs as part of the JCIDS coordination and acquisition milestone review process. Leverage material command acquisition intelligence inputs such as independent intelligence assessments (IIA) to develop certification recommendations.

2.10.4. Recommend ISR SAP capabilities for inclusion in and removal out of the IJSTO.

2.10.5. Manage SAP billet plans and other SAP security administration (i.e. AAA) activities for AF/A2 staff.

2.11. The Director, Cyberspace Operations (A3C/A6C), shall:

2.11.1. Serve as the principal advisor to SAF/CIO A6 for CIO-related issues for SAPs. Coordinate with SAF/AAZ to facilitate SAP accesses for the SAF/CIO A6 requirements (i.e. Clinger-Cohen Act certification).

2.11.2. Serve as the principal advisor to AF/A3/5 and SAF/CIO A6 for SAPs involving cyberspace operational capabilities.

2.12. The Division Chief, Special Programs Division (AF/A3O-OZ), shall:

2.12.1. Serve as a principal advisor to AF/A3/5 for SAP operations.

2.12.2. Serve as the CSAF's operational lead to organize, train and equip AF elements of the joint force with SAP capabilities and facilitate operational SAP integration across HQ USAF.

- 2.12.3. Serve as the primary AF focal point for IJSTO to the Joint Staff and other organizations working IJSTO.
- 2.12.4. Serve as the Air Force focal point with Joint Staff on adding or removing capabilities from IJSTO. Ensure appropriate coordination prior to submission to include, but not limited to the AF SAPCO, SPOC Executive Secretary, and SAF/GC prior to final Air Force approval and submission to the Joint Staff.
- 2.12.5. Serve as the lead Air Force office for the implementation of IJSTO common access billets (CAB). The Division Chief will approve the specific SAPs included in each AF sponsored CAB event.
- 2.12.6. Serve as the primary Air Force office managing the CW AMP. Submit proposals to the Director, AF SAPCO, to modify which SAPs are included in the CW AMP in coordination with appropriate OCA(s), the SPOC Executive Secretary and AF/A3/5.
- 2.12.7. Support all AF/A3 staff in coordinating and staffing SAP-related training plans and SAP test activity requests that require OSD approval.
- 2.13. Provide SAP GSSO support, billet management, and other SAP security administration (i.e. AAA) activities for all AF/A3 staff performing SAP activities.
- 2.14. The Division Chief, Program Integration Division (AF/A4/7PE), shall:
  - 2.14.1. Serve as the principal advisor to AF/A4/7 for SAPs.
  - 2.14.2. Support life-cycle sustainment for SAP acquisitions.
  - 2.14.3. Represent Air Force product support equities.
  - 2.14.4. Provide coordinated policy implementation guidance to Air Force logistics, installations and mission support activities.
- 2.15. The Director, Operational Capability Requirements, AF/A5R, shall:
  - 2.15.1. Serve as a principal advisor to AF/A3/5 for SAP operational capability requirements.
  - 2.15.2. Chairs, oversees and conducts the AF Requirements Oversight Council (AFROC) Special Session.
  - 2.15.3. AF/A5R(J) shall serve as the primary AF representative to the Joint Capabilities Board (JCB) and is the primary plus-one attendee to the JROC (VCSAF is the AF JROC principal) for all JCIDS topics, unless access constraints exist as determined by SAF/AAZ. In those cases where A5R(J), A5R, and A5R(D) cannot obtain the necessary access authority SAF/AAZ will normally pick-up these A5R(J) responsibilities.
  - 2.15.4. AF/A5R DOS tracks all classified operational capability requirements and represents cross command prioritization of those requirements in SPRG deliberations.
  - 2.15.5. AF/A5R DOS provides SAP GSSO support, billet management, and other SAP security administration (i.e. AAA) activities for all AF/A5 organizations performing SAP activities and AFROC Special Session principal members, as required.
  - 2.15.6. AF/A5R DOS shall serve as the primary AF/A5R representative for all SAP issues within AF/A5R.

- 2.16. The Division Chief, Program Integration Division (AF/A8P), shall:
- 2.16.1. Serve as the principal advisor to AF/A8 for SAPs.
  - 2.16.2. Supports the Planning, Programming, Budgeting and Execution (PPBE) submissions for SAPs.
  - 2.16.3. Provide inputs regarding the coordination of SAPs with strategic plans and long range concepts.
  - 2.16.4. Ensure AF representatives to the 3-Star Programmer's Review and SAP DMAG are prepared on SAP issues, in conjunction with the SPOC Executive Secretary.
  - 2.16.5. Prepare and present annual OSD PBR submissions to DCAPE and OUSD Comptroller, with SAF/AQL and SAF/FMBIB.
  - 2.16.6. Act as the focal point for the basing process of all SAPs through the Strategic Basing Executive Steering Group.
  - 2.16.7. Serve as the interface to the AF Corporate Board and coordinate with the SPOC Executive Secretary for day-to-day integration and de-confliction with the Air Force Corporate Board process prior to providing recommendations to the SPOC.
- 2.17. The Director, Force Structure Analyses (AF/A9F) shall:
- 2.17.1. Serve as the principal advisor to AF/A9 for SAPs.
  - 2.17.2. Advise the SPRG by providing SAP analyses to inform the PPBE process.
- 2.18. The Division Chief, Capabilities and Integration (AF/A10-C), shall serve as the principle advisor to the AF/A10 for all HAF nuclear matters involving SAPs.
- 2.19. The Division Chief, Special Programs Division (AF/TEZ), shall:
- 2.19.1. Serve as the principal advisor to AF/TE for SAPs regarding range policy and guidance, funding and infrastructure sustainment at test ranges. Serve as the primary functional lead for SAPs in which AF/TE has OCA.
  - 2.19.2. Ensure the necessary test infrastructure and personnel are available to support designated SAPs undergoing test and evaluation.
  - 2.19.3. Represent Air Force Operation and Test Evaluation Center (AFOTEC) on funding, resources, facilities, contracts, security, and training issues at the SPRG when appropriate.
  - 2.19.4. Serve as the lead for the Foreign Material Program (FMP) for SAPs.
  - 2.19.5. Provide SAP GSSO support and management for AF/TE SAP activities.
- 2.20. The Security Director, Air Force Office of Special Investigations, Office of Special Programs (AFOSI PJ), shall:
- 2.20.1. Serve as the principal advisor to SAF/IG for SAPs.
  - 2.20.2. Execute program security for SAPs.
  - 2.20.3. Act as the security classification manager for SAP SCGs to ensure horizontal protection and compliance with DoD and AF policy and endorse all SAP SCGs.

- 2.20.4. Provide AFOSI services to include program security, counterintelligence, counterespionage, major criminal investigations, technical security and countermeasure services, and other specialized AFOSI activities (e.g., polygraph and credibility assessment program).
- 2.20.5. Notify the Director, AF SAPCO, of any security inquiries or investigations which affect SAPs.
- 2.20.6. Implement a SAP security program to ensure comprehensive security management and execution.
- 2.20.7. Appoint a PSO, for each SAP, to be responsible for overall SAP security management IAW DoD guidance.
- 2.20.8. Evaluate contractors against security criteria when a carve out contract exists, through the head GCA and endorse all DD Forms 254, *Contract Security Classification Specification*, issued and associated with their assigned programs. PSOs must coordinate with the appropriate contracting officer (CO) and program manager (PM) to validate the DD Form 254 contains language indicating DSS is carved out of program oversight and identifies AFOSI PJ as having security and compliance inspection responsibility in accordance with the NISP. COs will finalize the DD254 only after endorsement by a PM and PSO. COs may not delegate the authority to approve DD254s for SAPs.
- 2.20.9. Ensure the Air Force Audit Agency (AFAA), Defense Contract Audit Agency (DCAA) and Defense Contract Management Agency (DCMA)'s requests for access are coordinated through the program office (specifically the CO) prior to submission to Security Director, AFOSI PJ.
- 2.20.10. Conduct security compliance inspections at all defense industrial base contractors where DSS has been carved out.
- 2.20.11. Provide a security and investigation trend analysis report at the start of each calendar year to the Director, AF SAPCO, and TIG which includes a summary of inspection trends, investigations, and security incidents.
- 2.20.12. Serve as the DAA for SAP ISs, when delegated by the SAF/AAZ.
- 2.20.13. Approve SAPFs for all SAP locations and all facility co-utilization (co-use) agreements or delegate approval authority to the responsible PSO.
- 2.20.14. Validate treaty notification and compliance requirements are adhered to for all SAPs.
- 2.20.15. Develop a CI support plan (CISP) for each SAP.
- 2.20.16. Evaluate Access Management Plans (AMPs) and/or billet plans ensuring adequate but limited accesses are available for senior leaders/executives and oversight personnel. The PSO will validate the Program Executive Officer (PEO) or equivalent and the CO have been coordinated with and agreed to any AMP or billet plan for programs still in the competition phase of acquisition.
- 2.20.17. Ensure all SAP security requests are endorsed by a PSO (i.e. AAAs, AAA delegations, AMPs, etc.) prior to SAF/AAZ review.

2.21. MAJCOM Commanders may provide a representative to advocate for MAJCOM requirements during the PPBE process for SAPs after coordination with the SPOC Executive Secretary and approval by the SECAF.

2.21.1. Commanders (MAJCOMs, DRUs, and FOAs) shall be responsible to:

2.21.2. Implement SAP security policies and conduct SAPs IAW all applicable laws, DoD and AF policy relating to/or governing SAPs and address security process issues with the PSO as applicable.

2.21.3. Ensure SAP security professionals and information assurance (IA) professionals are appointed to support all associated SAPs.

2.21.4. Ensure ISs are resourced, authorized by an approved DAA and supported by IA professionals trained IAW DoDD 8570.01.

2.21.5. Support MAJCOM IG in conducting SAP security compliance inspections, as required.

2.21.6. Ensure the PSO is notified of the location of all facilities which are executing SAPs.

2.21.7. Ensure current arms control and treaty compliance requirements, obligations, and constraints are implemented. All associated government and contractor facilities hosting SAP activities shall have site-specific treaty inspection plans that include detailed managed-access provisions. SAP activity treaty inspection readiness plans shall be approved by the PSO and are subject to annual review and certification. Develop and implement an education program for all participants, as required.

2.21.8. Manage SAP billet plans and other SAP security administration (i.e. AAA) activities. Obtain endorsement by a PSO for all security related actions or incidents prior submission to SAF/AAZ.

2.21.9. Implement a SAP SETA program.

2.21.10. Ensure PMs and PSOs endorse DD254s prior to CO's approval.

2.21.11. Support the development of SAP transition plans.

2.22. Acquisition Program Directors and PMs shall:

2.22.1. Ensure PMs and PSOs endorse DD254s prior to the CO's approval.

2.22.2. Ensure ISs are resourced, authorized by an approved DAA and supported by IA professionals trained IAW DoDD 8570.01.

2.22.3. Ensure the PSO is notified of the location of all facilities which are executing SAPs.

2.22.4. In conjunction with the PSO, ensure contractor compliance with contract security requirements.

2.23. For any SAP assigned to a Headquarters element, the organization shall provide a program element monitor (PEM) as the primary POC for coordination with the SPOC Executive Secretary. As a minimum, PEM responsibilities include: providing functional and subject matter expertise to the program; participation in program reviews; oversight of

funding execution; review and coordination of applicable program documentation; and executing tasks issued by the SPOC Executive Secretary, as required. PEMs will participate in SAP processes and the SAP governance structure.

2.24. The Commander, AFOTEC, shall:

2.24. (AFOTEC) The Director of Operations (AFOTEC/A-3) shall:

2.24.1. Serve as the Operational Test Agency (OTA) or provide support to the assigned OTA for Air Force acquisition category (ACAT) I, IA, II, OSD T&E Oversight, and multi-service SAP acquisition programs, as assigned.

2.24.1. (AFOTEC) Direct operations and processes that define and accomplish AFOTEC OT&E and OT&E-related activities of all SAP programs.

2.24.2. Advise AF/TEZ, SAF/AQL, and SAF/AAZ on funding, resources, facilities, contracts, security, and training issues for SAP systems undergoing operational test and evaluation.

2.25. (AFOTEC) The Division Chief, Special Access Programs Division (AFOTEC/A-3Z), shall:

2.25.1. (AFOTEC) Serve as the principal advisor to AFOTEC/A-3 for SAP OT&E execution, guidance, policy, and doctrine.

2.25.2. (AFOTEC) Serve as the OPR for all AFOTEC SAP operational test issues.

2.25.3. (AFOTEC) Provide operational requirements and priorities for SAP Security (AFOTEC/CVI SAP) and SAP IT (AFOTEC/A-6O SAP).

2.25.4. (AFOTEC) Provide oversight of operational test policy, management and execution for SAPs undergoing operational test by AFOTEC.

2.25.5. (AFOTEC) Provide staff support for all AFOTEC SAP programs IAW the AFOTECMAN 99-101.

2.25.6. (AFOTEC) Maintain status of SAP execution at Dets and OLs.

2.25.7. (AFOTEC) Be the designated Access Approval Authority (AAA) for AFOTEC SAP access. This AAA delegation may not be further delegated unless coordinated with the AFOTEC Commander and approved in writing by the Director, Security and Special Program Oversight (SAF/AAZ).

2.25.8. (AFOTEC) Update AFOTECs SAP billet plan annually, in coordination with AFOTEC Detachments and Directorates.

2.26. (AFOTEC) The AFOTEC/A-3Z (Technical Advisor, SAP) shall:

2.26.1. (AFOTEC) Provide technical advice and consultation for SAP programs to the director, deputy director, Dets, OLs, and others as requested.

2.26.2. (AFOTEC) Serve as the focal point for scientific and technical issues concerning all phases of OT&E in support of SAPs.

2.26.3. (AFOTEC) Coordinate operational analysis and engineering support for SAPs.

2.26.4. (AFOTEC) Provide technical assistance to and oversight of SAPs at the HQ, Dets, and OLs.

2.27. (AFOTEC) AFOTEC/A-3Z (Resource Management, SAP) shall:

2.27.1. (AFOTEC) Function as the headquarters staff test resource manager (TRM) for AFOTEC SAP programs.

2.27.2. (AFOTEC) Perform facility, contract, and financial oversight of AFOTEC SAP programs.

2.27.3. (AFOTEC) Develop and prepare short- and long-range (5-/10-year) planning guidance, in coordination with the Det TRMs that complies with broad agency programs and policies for SAP programs.

2.27.4. (AFOTEC) Execute policies and procedures to maintain financial integrity and compliance with public law, DoD directives, and Air Force instructions.

2.27.5. (AFOTEC) Provide budget and test resource advice for Det test teams, OLs, and Det test resource managers.

2.27.6. (AFOTEC) Advise the director, deputy director for SAP, Dets, OLs, HQ USAF/TEZ, SAF/AQL, SAF/AAZ, and special programs offices on funding, resources, facilities, contracts, and training issues.

2.27.7. (AFOTEC) Review all SAP test resource plans IAW AFOTECMAN 99-101.

2.27.8. (AFOTEC) Coordinate memorandums of agreement for AFOTEC SAPs.

2.28. (AFOTEC) AFOTEC/A-6O (SAP Information Technology (IT) support) shall:

2.28.1. (AFOTEC) Provide IT oversight to all AFOTEC entities processing SAP material.

2.28.2. (AFOTEC) Support all AFOTEC SAP IT systems at Kirtland Air Force Base, New Mexico.

2.28.2.1. (AFOTEC) Assign an Information System Security Officer/Information System Security Manager (ISSO/ISSM) to handle their respective organization's SAP IT-related issues. ISSM/ISSO responsibilities are identified in Joint Special Access Program Implementation Guide (JSIG) and the Intelligence Community Directive (ICD) 503.

2.28.2.2. (AFOTEC) Ensure ISSM/ISSOs/IT personnel are qualified to perform their duties. Make funds available to obtain appropriate training.

2.28.3. (AFOTEC) Coordinate with the AFOTEC program security officer (PSO) to acquire authority-to-operate/authority-to-connect (ATO/ATC) or external information system approval for every SAP IT system at Kirtland Air Force Base prior to their installation and use.

2.28.4. (AFOTEC) Ensure Dets/OLs obtain proper ATO/ATC or EIS approval from the AFOTEC PSO for all IT systems prior to installation and processing.

2.28.5. (AFOTEC) Develop, maintain, and enforce the Information Assurance Standard Operating Procedures (IA SOP) supporting SAPs at Kirtland Air Force Base.

- 2.28.6. (AFOTEC) Review and coordinate IA SOP's developed at Dets/OLs.
  - 2.28.7. (AFOTEC) Provide SAP IT training, assistance, and guidance to program-cleared personnel assigned to Kirtland Air Force Base.
  - 2.28.8. (AFOTEC) Conduct annual SAP IT self-assessments within AFOTEC SAP facilities at Kirtland Air Force Base.
  - 2.28.9. (AFOTEC) Conduct biennial SAP IT inspections at AFOTEC Dets and OLs.
  - 2.28.10. (AFOTEC) Suggest training for the Det/OL ISSO/ISSM.
- 2.29. (AFOTEC) AFOTEC/CVI (SAP Security) shall:
- 2.29.1. (AFOTEC) Serve as the focal point for issues related to SAP security policies, procedures, administration, information, industrial, personnel, physical, and operational security.
  - 2.29.2. (AFOTEC) Develop SOP for HQ special access program facilities (SAPF).
    - 2.29.2.1. (AFOTEC) Review and coordinate Det/OL SOPs with AFOSI/PJ Det 8 OL-A PSO for approval.
  - 2.29.3. (AFOTEC) Process program access requests (PAR) for SAP accesses for AFOTEC-assigned personnel.
    - 2.29.3.1. (AFOTEC) Conduct indoctrination briefings/debriefings for HQ AFOTEC personnel IAW applicable program briefings and security classification guides.
    - 2.29.3.2. (AFOTEC) Provide courtesy indoctrinations/debriefings, when requested.
    - 2.29.3.3. (AFOTEC) Notify Det/OL Government SAP Security Officer's (GSSO) upon approval of PARs.
    - 2.29.3.4. (AFOTEC) Update/maintain the letter of X's and the Joint Access Database Enterprise (JADE).
  - 2.29.4. (AFOTEC) Administer quarterly SAP Security Education Training and Awareness (SETA) and OPSEC training to HQ AFOTEC program-cleared personnel.
    - 2.29.4.1. (AFOTEC) Provide Det/OL GSSOs with quarterly SETA briefings.
  - 2.29.5. (AFOTEC) Develop an OPSEC plan and critical program information (CPI) briefing to HQ AFOTEC program-cleared personnel.
    - 2.29.5.1. (AFOTEC) Provide Det/OL GSSOs with annual updates to the HQ AFOTEC OPSEC plan and CPI briefings.
  - 2.29.6. (AFOTEC) Process all aspects of HQ AFOTEC SAP security administration paperwork through AFOSI/PJ Det 8 OL-A (AFOTEC PSO).
    - 2.29.6.1. (AFOTEC) Review and acts as the liaison to AFOSI/PJ Det 8 OL-A PSO for all Det/OL SAP security administration paperwork, unless outlined in an agreement between the AFOSI/PJ Det 8 OL-A PSO and an area PSO (APSO).
  - 2.29.7. (AFOTEC) Conduct annual SAP security self-assessments for HQ AFOTEC SAPFs and biennial security inspections for AFOTEC Dets/OLs.

- 2.29.7.1. (AFOTEC) Coordinate with AFOSI/PJ Det 8 OL-A PSO to validate the most current security inspection checklist and special emphasis items (SEI). (Note: SEIs are subject to change annually and are designated by the AFSAPCO).
- 2.29.7.2. (AFOTEC) Ensure self-assessment checklist items and SEIs are reported accurately. (For example: a YES response indicates compliance of the item, and must include how it is applicable and the dates/locations of appointment letters, memos, etc.; a NO response indicates non-compliance and what corrective actions should be taken; and a NOT APPLICABLE (N/A) response indicates that the item is not required for that program and explain why or why not).
- 2.29.7.3. (AFOTEC) Ensure the HQ self-assessment report and Det/OL self-assessment reports are written to accurately identify each deficiency as a finding, deviation, and/or government action item (GAI). Each finding and deviation must include a corrective-action plan and a projected date for when the deficiency will be corrected, which should not exceed 30 days from the date of the self-assessment report. If more than 30 days is required to correct the deficiency, a brief justification must be included, and a follow-up report must be accomplished every 30 days until the deficiency is closed by AFOSI/PJ Det 8 OL-A PSO.
- 2.29.7.4. (AFOTEC) Ensure HQ's self-assessment reports and Det/OL self-assessment reports are forwarded to AFOSI/PJ Det 8 OL-A PSO for review/closure.
- 2.29.7.5. (AFOTEC) Coordinate with other DoD and MAJCOM GSSOs to produce one comprehensive security inspection, when applicable.
- 2.29.8. (AFOTEC) Act as the single point-of-contact for SAP-related inquiries and investigations involving AFOTEC program-cleared personnel and provide assistance to Det/OL GSSOs.
- 2.29.8.1. (AFOTEC) Ensure SAP-related inquiries and investigations are reported to the AFOSI/PJ Det 8 OL-A PSO within 24 hours.
- 2.29.8.2. (AFOTEC) Ensure SAP-related inquiries and investigations are completed within 10 duty days and forwarded to AFOSI/PJ Det 8 OL-A for closure.
- 2.29.9. (AFOTEC) Review contractor statements of work, delivery orders, and/or facility construction plans, if required.
- 2.29.10. (AFOTEC) Review and coordinate DD Forms 254 for contractors that directly support the AFOTEC SAP portfolio.
- 2.29.10.1. (AFOTEC) Submit DD Forms 254 to AFOSI/PJ Det 8 OL-A PSO for approval. (Note: AFOSI/PJ Det 8 OL-A PSO approval is required prior to the conduct of any SAP work).
- 2.30. (AFOTEC) Detachments and Operating Locations shall:
- 2.30.1. (AFOTEC) Inform AFOTEC/A-3Z when outside organizations request AFOTEC's involvement on SAPs.
- 2.30.2. (AFOTEC) Process PARs through AFOTEC/CVI-SAP Security, unless AAA has been granted.

- 2.30.2.1. (AFOTEC) Conduct indoctrination briefings/debriefings to program-cleared personnel IAW applicable program briefings and security classification guides.
- 2.30.2.2. (AFOTEC) Forward indoctrination briefing/debriefing paperwork to AFOTEC/CVI SAP Security within 24 hours.
- 2.30.2.3. (AFOTEC) Provide courtesy indoctrination/debriefings, when requested.
- 2.30.3. (AFOTEC) Administer quarterly SAP SETA, OPSEC training, and CPI briefing to program-cleared personnel and forward results to AFOTEC/CVI SAP Security.
- 2.30.4. (AFOTEC) Conduct an annual SAP security self-assessment and forward the self-assessment report to AFOTEC/CVI SAP Security for review/coordination.
- 2.30.4.1. (AFOTEC) Ensure self-assessment checklist items and SEIs are reported accurately. (For example: A “Yes” response indicates compliance of the item, and must include how it is applicable and the dates/locations of appointment letters, memos, etc.; a NO response indicates non-compliance and what corrective actions should be taken; and a NOT APPLICABLE (N/A) response indicates that the item is not required for that program and explain why or why not).
- 2.30.4.2. (AFOTEC) Ensure the self-assessment reports are written to accurately identify each deficiency as a finding, deviation, and/or GAI. Each finding and deviation must include a corrective-action plan and a projected date for when the deficiency will be corrected, which should not exceed 30 days from the date of the self-assessment report. If more than 30 days is required to correct the deficiency, a brief justification must be included, and a follow-up report must be accomplished every 30 days until the deficiency is closed by AFOSI/PJ Det 8 OL-A PSO. Self-assessment reports must be signed by the Det CC or OL Chief.
- 2.30.5. (AFOTEC) Promptly report SAP-related inquiries and investigations that involve AFOTEC program-cleared personnel to AFOTEC/CVI SAP Security. Note: Det/OL GSSOs may utilize APSOs for SAP related inquiries and investigations involving AFOTEC program-cleared personnel, only if the SAP-related inquiry/incident occurred in a non-AFOTEC owned facility or otherwise directed by AFOSI/PJ Det 8 PSO.
- 2.30.5.1. (AFOTEC) Ensure SAP-related inquiries and investigations are completed within 10 duty days and forwarded to AFOTEC/CVI SAP Security for review/coordination.
- 2.30.6. (AFOTEC) Review contractor statements of work, delivery orders, and/or facility construction plans, if required.
- 2.30.7. (AFOTEC) Review DD Forms 254 for contractors that directly support AFOTEC SAPs.
- 2.30.7.1. (AFOTEC) Act as a liaison between the APSO and the AFOTEC PSO.
- 2.30.7.2. (AFOTEC) Develop SOPs, IA SOPs, Fixed Facility Checklists, accreditation letters, OPSEC plans, and other related documentation for their respective organization and coordinate the documentation through the AFOTEC/A-6 SAP IT staff and/or CVI SAP Security, as applicable.

2.30.7.3. (AFOTEC) Assign an ISSM/ISSO to handle their respective organization's SAP IT-related issues. ISSM/ISSO responsibilities are identified in JSIG and the Intelligence Community Directive (ICD) 503.

2.30.7.4. (AFOTEC) Ensure ISSM/ISSOs/IT personnel are qualified to perform their duties. Make funds available to obtain appropriate training.

2.30.7.5. (AFOTEC) Develop and coordinate fixed-facility checklists, facility accreditations, and certifications for SAP secure work areas and computer processing.

### **3. SAP Governance.**

3.1. The SPRG serves as the advisory panel to the SPOC and Special Programs Review Board (SPRB) and is responsible for integration of requirements and recommends allocation of resources across the SAP portfolio. The resource allocation process starts with identifying requirements from the Air Force Requirements Oversight Council (AFROC), MAJCOMs and other organizations. The SPRG develops the Air Force SAP Integrated Priority List (IPL), matches available resources to requirements and make recommendations to the SPOC for the POM, Budget Estimate Submission (BES), and the President's Budget (PB). The SPRB meets to review the SPRG and the Air Force Corporate structure recommendations to ensure de-confliction of the overall Air Force budget. Following the SPRB, the SPOC Executive Secretary presents the budget recommendation to the SPOC for final approval. The SPRG is chaired by the Director, SAF/AQL. The SPRG is co-chaired by SAF/AQL and AF/A8PE when conducted for the purpose of POM deliberation.

3.2. The SPRG members are SAF/AAZ, SAF/AQSC, SAF/FMBIB, AF/A1M, AF/A2Z, AF/A3O-OZ, AF/4/7PE, AF/A5R-DoS, AF/A8PE, AF/TEZ and AFRCO and designated MAJCOM representatives. Advisors to the SPRG are SAF/AQCS, SAF/AQR, SAF/GCI, AF/A3C/A6C, AF/A8X, AF/A9F, AF/A10-C, AFOSI PJ, AFAA/AGS, and SAF/IGI Special topic advisors will be invited as required by SPRG Chair.

3.3. The SPRB is primarily responsible for ensuring integration of SAP and non-SAP programmatic adjustments proposed during budget deliberations. In this role, the SPRB will make recommendations to the SPRG on any actions required to ensure integration of SAP and non-SAP programs prior to budget recommendation submission to the SPOC. The SPRB is co-chaired by AF/A8P and SAF/AQX. SPRB members include SAF/AAZ, SAF/FMB, AF/A2R, AF/A3O, AF/A5R, AF/A8X, AF/TEZ, designated MAJCOM representatives, and any appropriately cleared AF Corporate Board member as approved by AF/A8P.

### **4. SAP Management, Administration and Oversight.**

4.1. General. Critical research and program technologies, systems, and information must be protected to prevent compromises that could significantly impact cost, schedule, performance, and supportability; affect program direction; degrade systems capabilities; shorten the life of the system; allow alteration of system capability; lead to technology transfer; or require additional resources to develop alternative countermeasures. Commands shall evaluate, plan and program for technology and program protection requirements from operational mission area planning until the system is demilitarized.

4.1.1. Security is a fundamental element of systems acquisition, cost, schedule, performance, and supportability. HAF, MAJCOMs, DRUs, and FOAs shall evaluate, plan, and program for technology and program protection requirements and supporting resources from the time mission area planning is conducted, throughout each life-cycle phase, until the system is demilitarized or approved for public release.

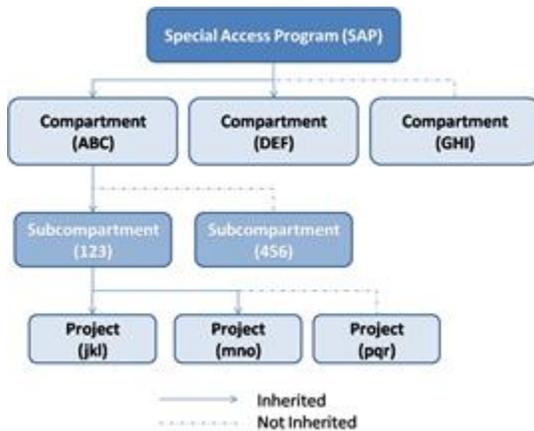
4.1.2. Commanders, Program Directors, and PMs shall plan and program for protection requirements as needed during the appropriate phases of the acquisition life-cycle for systems with or without a weapon system security standard, normally through the Future Year Defense Plan (FYDP). Security protection requirements shall be identified in needs and requirements documentation provided to the implementing, supporting, and participating commands to counter threats against Critical Program Information (CPI) and Critical Components (CC). SAF/AAZ shall be notified of any cover employment requirements during any phase of the SAP life cycle. In coordination with the program manager PSOs shall coordinate life-cycle physical security standards with the operational command(s) no later than entry into Milestone B, and at each major program milestone thereafter. This coordination will include an analysis of CPI and CC with Air Force Red Team, AFOSI, and AF/A2. The PSOs shall develop cost-effective protection alternatives and countermeasures to protect CPI and CC at all locations as determined by the risk.

4.1.3. PMs shall integrate protection technologies through the principles of systems security engineering (SSE). Life-cycle systems security support shall identify time-phased affordable security protection alternatives and requirements, integrating them into a weapon system and supporting subsystems security architecture, other required equipment, and supporting facilities using risk management principles based on valid threat information.

4.1.4. SAPs shall develop a transition plan that addresses the employment of the operational capability without SAP enhanced security protections. The transition plan will be developed from the transition strategies that guide the SAP protection levels throughout each major program milestone.

4.2. SAP Hierarchy. The fundamental structure of a special access program has four levels. The highest level is the SAP, the 2<sup>nd</sup> level is called a compartment, the 3<sup>rd</sup> level is called a sub-compartment, and the 4<sup>th</sup> level is called a project. Figure 1 reflects a visual representation of this structure. This structure is reflected in AFADS. By default, lower levels components are inherited from the next higher level. Exceptions, for which lower level components are not inherited from the higher level, must be approved by the AF SAPCO at the time of establishment. As each component is approved, the inheritance, as well as, the nickname and/or code word and PID are entered into AFADS. Personnel being briefed to compartments, sub-compartment, or projects will only be told they are being briefed into a "SAP" in order to protect the actual level of information being presented.

**Figure 1. Notional SAP Security Architecture**



4.3. PSAP Process. The DepSecDef has delegated the authority for establishment of PSAPs to the Director AF SAPCO. DoDI 5205.11 outlines the PSAP approval process and lists the required elements of a PSAP package. In addition to these required elements, all PSAP requests shall include a transition plan. Upon PSAP approval, enhanced security measures may be applied for a period not to exceed 210 days. If the PSAP is approved by the SecDef or DepSecDef notification is provided to Congress. The PSAP becomes a SAP after a period of 30 days has elapsed after notification to Congress

4.4. Establishment of Compartments, Sub-compartments and Projects. Prior to the establishment of new compartments, sub-compartments or projects, a thorough review of existing elements must be accomplished to mitigate the occurrence of redundant and unnecessary compartments, sub-compartments, and projects.

4.4.1. After the review is complete and a determination has been made that a new compartment, sub-compartment or project is required, a registration request shall be submitted to SAF/AAZ to reserve and de-conflict the PID and nickname with NICKA, AFADS, and DCADS (or successors). This initial request must also indicate if the compartment, sub-compartment or project shall be an apportioned capability. The AF SAPCO shall provide, in writing, the approved and registered nickname, PID and code word, as required.

4.4.2. The written request to establish a compartment, sub-compartment, or project shall be submitted to SAF/AAZ for approval. The establishment request shall include the following:

**Table 1. Establishment Request Required Elements**

Scope (two line description)
Hierarchy
Level (compartment, sub-compartment or project)
Inheritance (default is inherited, if not provide justification)
Classification Level (S, TS, or both)
OSD Oversight Category (acquisition, intelligence, or operations and support; must be the same as the SAP)
Type (acknowledged, unacknowledged)

PEM
PSO
Funding Source (content only or funded)
Billeted (yes or no; required for waived programs)
Approved SCG

4.4.3. With the approval of an establishment memorandum by SAF/AAZ the nickname and PID shall be entered into AFADS and DCADS for use.

4.4.4. On a case-by-case basis, when a time-critical requirement exists to establish a compartment, sub-compartment, or project, a SAP OCA may use as an interim solution, a memorandum for classification guidance. The memorandum shall address the essential elements required in an SCG and shall be endorsed by the Security Director, AFOSI PJ. SCGs must be approved and submitted to SAF/AAZ within 90 days of compartment, sub-compartment, or project initiation.

4.5. SAP Management, Administration, and Oversight. After approval of the proposed changes by the SECAF, the AF SAPCO shall notify the Director, DoD SAPCO, in writing of any following proposed changes. The AF SAPCO shall also notify the DoD SAPCO of approvals for additions or changes of nicknames, code words or PIDs for compartments, sub-compartments or projects.

4.5.1. Notification of change of OSD Category (acquisition, intelligence, or operations and support) requires:

4.5.1.1. Memorandum with the justification for the change from the SECAF

4.5.1.2. Quad chart

4.5.1.3. Draft DepSecDef memorandum

4.5.2. Notification of change of type (acknowledged, unacknowledged, and waived) requires:

4.5.2.1. Memorandum with the justification for the change from the SECAF

4.5.2.2. Quad Chart

4.5.2.3. Threat Assessment

4.5.2.4. Draft revised SCG

4.5.2.5. PA Plan

4.5.2.6. Draft DepSecDef and Congressional memorandums

4.5.3. Notification of alteration of scope requires:

4.5.3.1. Memorandum with the justification for the change from the SECAF

4.5.3.2. Quad Chart

4.5.3.3. Draft revised SCG

4.5.3.4. Draft DepSecDef and Congressional memorandums

4.5.4. Notification of IJSTO apportionment or deapportionment requires that AF SAPCO provide a copy of the AF/A3/5 apportionment or deapportionment approval.

4.5.5. Notification of termination of a SAP requires:

4.5.5.1. Memorandum with the justification for the change from the SECAF

4.5.5.2. Quad Chart

4.5.5.3. Disestablishment Plan

4.5.5.4. Draft DepSecDef and Congressional memorandums

4.5.6. Notification of transition of a SAP requires:

4.5.6.1. Memorandum with the justification for the change from the SECAF

4.5.6.2. Quad Chart

4.5.6.3. Threat Assessment

4.5.6.4. Draft revised SCG

4.5.6.4.1. PA Plan

4.5.6.5. Transition Plan

4.5.6.6. Legal Review

4.5.6.7. Draft DepSecDef memorandum

4.5.7. Notification of support of non-DoD SAPs requires AF SAPCO provide a copy of the MOA between the AF and outside organization.

4.5.8. Notifications of proposals to relieve DSS of NISP security oversight responsibilities (carve out) requires:

4.5.8.1. Memorandum with the justification from the SECAF

4.5.8.2. Draft DepSecDef memorandum

4.5.9. Notification of proposal for foreign involvement requires:

4.5.9.1. Memorandum with the justification from the SECAF

4.5.9.2. Quad Chart

4.5.9.3. Threat Assessment

4.5.9.4. Draft DepSecDef memorandum

4.6. SAP Directive (SAPD). The SAPD conveys specific SAP guidance, decision authority and identifies the various organizations along with their essential responsibility for executing a successful SAP. It provides a source document for the program. SAPDs are required for funded SAPs with a requirement to receive Headquarters direction for execution. The SAPD should be reviewed annually and updated as required. All SAPDs will be formally updated (i.e. re-coordinated) every five years. SAF/AQL is responsible for oversight and management of SAPDs.

4.7. Access Management Plans (AMPs). In order to facilitate access to multiple SAPs for a defined group of personnel for a specific function, an access management plan may be established. A specific nomenclature is defined to indicate a set of SAPs. AMPs are used to streamline access to programs. When approved for an AMP, personnel are approved for all the SAPs identified as part of the AMP and will sign a program indoctrination agreement (PIA) for the consolidated set of SAPs in the AMP. Some AMPs apply restrictions as to when and how the accesses may be used (e.g. CW) and these restrictions will be documented in the AMP. All AMPs, and modifications, must be coordinated by the OCA(s), endorsed by a PSO, and approved by SAF/AAZ. AMPs shall also have a billet plan including billet numbers for tracking in AFADS. AMP nomenclatures should never be used as classification markings for SAP information or on SAP indoctrination agreements. AMPs must address the following areas:

- 4.7.1. The specific function the AMP supports.
- 4.7.2. The specific SAPs that are part of the AMP.
- 4.7.3. The specific personnel that the AMP applies to.
- 4.7.4. The OPR for execution of the AMP.
- 4.7.5. A billet plan.

4.8. Billet Plans. Billet plans are a tool for access approval authorities to document access requirements by position for an organization. AAAs may approve billet plans for those programs for which they have AAA after endorsement by a PSO. All approved billet plans must be forwarded to SAF/AAZ. Billet numbers must be entered into AFADS, or approved database. Billet plans are required for all waived SAPs.

4.9. SAP Support to War-games or Exercises. All war-game or exercise activity, that has a requirement to incorporate SAP(s) as part of the activity, must provide the information in Table 2 to AF SAPCO at least 120 days prior to the event:

**Table 2. Information required for Request for SAP Inclusion in War-games or Exercises**

Terms of Reference or Concept of Operations
Proposed billet plan
Justification for each proposed SAP
Identification of the lead GSSO support
How long the access(es) is required
Proposed schedule
Level of SAP participation (S or TS)

- 4.9.1. SAF/AAZ will provide written approval, after coordination with all OCAs, indicating the implementation details of the approval.
- 4.9.2. Once approved, each OCA shall provide subject matter experts to support, as available.
- 4.9.3. Events utilizing COAL WARFIGHTER Cat A billets or IJSTO CABs shall follow approved guidelines as outlined in the Air Force COAL WARFIGHTER Security Management Plan or the IJSTO Air Force CAB Security Management Plan.

4.10. Program Protection Plans (PPPs). SAP PMs must develop PPPs or an alternative document that combines program protection and other aspects of program security. If a PPP is not developed, all of the topics reflected below are required to be considered during the entire life of SAPs (i.e. during program reviews) and must be identifiable in existing documentation.

**Table 3. Program Protection Elements**

Technology description	Security Classification Guide(s)
Program information	System security engineering considerations (risk mitigation)
Identification of CPI and CC	Supply chain risk management
Disclosure considerations as applicable to the Freedom of Information Act (FOIA), unclassified technical data from public disclosure and PII data	Command, control, communication, computers, and intelligence (C4I) certification and accreditation
Threats to CPI and CC	Countermeasures
Vulnerability of CPI and CC to the threats	Anti-tamper plan
Technology Assessment/Control Plan, if required	Information assurance/network security strategy; cyber security
Horizontal protection of CPI and CC	Test protection planning
Identification of Critical Technology Elements or Components	Independent verification & validation (IV&V) of ISs, as required
Foreign disclosure and involvement	Defense exportability features
Counterintelligence support plan	Foreign sales and co-production
Monitoring and reporting compromises	Demilitarization
Intelligence, surveillance and reconnaissance requirements and supportability	Follow-on support and modification management
Operations Security (OPSEC) plan, if required	Treaty inspection readiness plans
Cryptographic support	Transition Plan

4.11. Test Approval Process. All test approval packages that require OSD approval shall be coordinated, at a minimum, by SAF/AAZ and SAF/GCI.

4.12. JCIDS Process (FCB, JCB & JROC Process). SAF/AAZ will serve as the single AF focal point for liaison with the JS J8 SAPCO for all SAP JCIDS topics/events and shall coordinate with AF/A5R, SAF/AQL and others, as appropriate, to ensure AF personnel are prepared to support Functional Capabilities Board (FCB), JCB and JROC activities. SAF/AAZ will facilitate and approve SAP access for all Air Force and non-Air Force representatives supporting the FCB, JCB and JROC processes for those SAPs which the Air Force has CA. SAF/AAZ will provide the JS J8 SAPCO the names of cleared attendees for all JCIDS SAP topics. SAF/AAZ will normally represent the AF at SAP JCB events in cases where AF/A5R(D) is not cleared. All AF representatives identified to support the JCIDS process will be trained IAW AFI 10-601.

4.13. Clinger-Cohen Act (CCA) Public Law 104-106 Certification. SAF/AAZ shall facilitate SAP accesses for SAF/CIO to support SAPs that require CCA certification. SAF/AAZ shall maintain a record of all approved SAP CCA certifications.

4.14. Release of SAP information to Foreign Nationals. Upon approval by SecDef or DepSecDef to release SAP information to a foreign national, SAF/IAP in coordination with the appropriate SAP OCA shall provide guidance for foreign disclosure officers for implementation.

4.15. Inter-service and Intra-governmental Support. The AF shall comply with DoDI 4000.19 for inter-service and intra-governmental support agreements, as required.

4.16. SAP Validation – SAP Oversight Review Board (SORB). The SORB shall validate compliance with all regulatory and statutory requirements for all SAPs. These validation reviews may be accomplished by either formal presentations to the SORB or an assessment of the information provided by the program executive officer (PEO) or PM. The SORB chair is responsible for informing the SECAF and appropriate SPOC members of the results of this board. Membership of the SORB consists of the principal member from SAF/AAZ, SAF/AAH, SAF/AQL, SAF/AQCS, SAF/FMBIB, SAF/GCI, SAF/IGI, AF/A2Z, AF/A3O-OZ, AF/TEZ, AFOSI PJ and advisors, as required. The SORB shall issue an assessment of SAP compliance with corrective actions for those areas when issues are identified.

4.17. SAP Annual Report to Congress. The DoD SAPCO provides specific guidance on the SAP report submission requirements, annually. The SAP annual report shall summarize all compartments, sub-compartments, and projects. In addition, the program hierarchy structure for each SAP program included in the SAP annual report to Congress must clearly be defined. The hierarchy elements of each SAP's structure shall be clearly displayed. The final Air Force portion of the SAP annual report, along with associated information, shall be staffed through SAF/AA, SAF/GC, SAF/FM, and AF/A8 prior to SECAF approval. The Air Force portion of the SAP annual report shall be submitted to the Director, DoD SAPCO by the AF SAPCO for coordination with the SRG and SAPOC before submission to the DepSecDef. The complete DoD SAP annual report will be provided to Congress by the DoD SAPCO.

4.18. Apportionment of SAP Capabilities Into or Out of IJSTO. SAP capabilities should be nominated to be apportioned into IJSTO when they are deemed operationally relevant and shall be nominated for apportionment after they have demonstrated operational capability or no later than (NLT) 18 months prior to planned initial operational capability (IOC), whichever occurs first. All OCAs shall submit an IJSTO capabilities package including items described below. In addition, the OCA for the capability must get approval from SecDef or DepSecDef to release to foreign nationals prior to submitting into IJSTO, if required. After AF/A3/5 approval of the apportionment package, the package shall be submitted to J39 for apportionment.

4.18.1. When submitting a SAP capability for apportionment the package must contain:

**Table 4. IJSTO Apportionment Package Requirements**

A program quad chart
A program fact sheet
An indoctrination briefing
A security classification guide (SCG)
A legal review
New nickname and PID (digraph or trigraph only) **
Identification of capability status
Recommendation for appropriate IJSTO billet structure
Recommendation on requirement for the review and approval process (RAP)
Recommendation of the deployment and execution authority
Recommendation of coalition releasability
Recommendation of inclusion in CW
** If the entire program is being apportioned there is no need to create a new nickname or PID.

4.18.2. If the capability is to be releasable to the coalition via IJSTO, the capability must be approved by DepSecDef for releasability, to the coalition, prior to the submission into IJSTO. In addition, the documents listed in Table 4, must be marked appropriately to reflect the approved releasability.

4.18.3. The documents submitted shall include sufficient information to facilitate COCOM planning efforts and contribute to an approved concept of operations.

4.18.4. The package for each capability shall be updated annually by the OCA, coordinated with SAF/AAZ, the SPOC Executive Secretary and forwarded AF/A3O-OZ on 1 Feb of each year. OCAs are encouraged to coordinate with AF/A3O-OZ prior to the submission.

4.18.5. Once a capability has been apportioned into IJSTO, all requests to change the status of the capability shall be coordinated with SAF/AAZ and upon approval by the AF/A3/5 shall be submitted to Joint Staff.

4.18.6. When a SAP, compartment, sub-compartment, or project has been apportioned into IJSTO, it must be reported in the SAP annual report to Congress until it has formally been removed from IJSTO.

4.18.7. The AF SAPCO may submit requests for waivers to this policy to Director, DoD SAPCO, for SRG consideration.

4.18.8. When a capability in IJSTO is no longer available, the OCA must coordinate with SAF/AAZ and submit a request to the AF/A3/5 to have it removed from IJSTO. The following items must be addressed in the request:

4.18.8.1. Name of the SAP/compartment/sub-compartment/project.

4.18.8.2. Disposition of the information (hardcopy, softcopy, hardware).

4.18.8.3. Justification of why the capability is no longer required in IJSTO (i.e. capability no longer available, capability no longer requires SAP security protections, etc.)

4.19. SAP Disestablishment (Disestablishment and/or Transition): A SAP disestablishment plan shall be developed when the SECAF elects to propose to terminate, cancel, or transition a SAP. The Director, AF SAPCO, shall approve the disestablishment plan. The disestablishment plan shall address:

**Table 5. Disestablishment Plan Elements**

<b>SECURITY AREAS</b>	<b>ADMINISTRATIVE ACTIONS</b>
Information Security	Contracting
Operations Security	Fiscal
Personnel Security	Audit
Physical Security	Property disposition
Industrial Security	Classified material disposition
Computer Security	Training
Communications Security	Public affairs
Security Classification Guidance	Legal
Downgrading Instructions	Logistics and Technical Support
Processes Applicable During and After SAP Disestablishment	Verification That Any Outstanding Patents Have Been Appropriately Classified
Threat Assessment	

4.19.1. The AF SAPCO shall provide the disestablishment plan to the Director, DoD SAPCO. The Director, DoD SAPCO, shall provide the disestablishment plan to the SAP Senior Working Group (SSWG) for review and determination for any potential impact on other programs.

4.19.2. The Director, DoD SAPCO, prepares the action memo for DepSecDef approval and prepares DepSecDef congressional notification letters for signature and notification to Congress.

4.19.3. Program termination is the action taken when the SAP programmatic activity is terminated. Termination is complete when no further expenditure of funds, no current contracts exist (period of performance has lapsed), and the information protected is no longer actively being utilized.

4.19.3.1. The information may be retained in its original form and the appropriate documents disposed of according to records management policy. The disestablishment plan must address the disposition of the information (i.e. continue with archiving, declassify or destroy material or transfer to another SAP, etc.).

4.19.3.2. The information may be transitioned as described below:

4.19.3.2.1. The information retains its classification, but without any enhanced SAP security measures.

4.19.3.2.2. The information is transitioned (no longer requiring enhanced security measures) to collateral or unclassified status. A PPP or technology protection plan (TPP) shall be required.

4.19.3.2.3. The information has been determined to be reclassified – such as TOP SECRET to SECRET or to UNCLASSIFIED.

4.19.3.2.4. The information retains its classification, but is transferred to another SAP.

4.19.3.2.5. The information retains classification, but changes SAP type or category.

4.20. Disestablishment of Compartments, Sub-compartments and Projects. Prior to the disestablishment of compartments, sub-compartments or projects, a thorough review of the program shall be conducted to ensure no further expenditure of funds, no current contracts exist, and the information is no longer actively being utilized. The annual SAP report shall indicate the final status of all compartments, sub-compartments, or projects as inactive. No further reporting to Congress is required if no further activity occurs.

## 5. Support to Non-AF SAPs.

5.1. Executing a SAP for Another DoD Component or Agency. The SECAF shall approve all requests from another DoD component or agency to execute their SAP (also includes compartments, sub-compartment or projects) on their behalf, including when the Air Force acts as the Executive Agent (EA). Non-AF entities the SECAF has approved for SAP support must agree to comply with this AFI and other AF guidance as applicable to SAPs, any exceptions will be captured in the MOA. The AF SAPCO will ensure those with acquisition, contracting, fiscal, legal, manpower, operational and security responsibilities, at a minimum, are briefed to the SAP(s) in order to coordinate and provide Air Force support to non-AF SAPs. Additionally, the AF SAPCO will inform DoD SAPCO of proposed new work for DoD SAPCO situational awareness and coordination. Activities currently being supported for a non-AF entity, prior to the approval of this document, must comply prior to accepting additional funding. The SECAF shall approve an MOA outlining the items in Table 6. MOAs must be updated or recertified, in writing, every five years.

**Table 6. Items Required in MOA For SAPs Directed By Another DoD Component or Agency**

Roles and responsibilities	Cognizant Security Authority (CSA) Oversight
Identify the Air Force OPR	Development of SCG; identification of the OCA
Identify the contracting office*	Funding or other resources
Period of agreement	Safety
Outline the Air Force's involvement	Interoperability – Operations/Logistics
Security	OPSEC
Access requirements/approvals	Testing plan
Accreditations and co-use	Legal review

agreements	
Reciprocity statement	Training plan
Resources*	Contracting review*
* Specific requirements and necessary resources will be determined in a separate support agreement at the base level with coordination/approval from the appropriate MAJCOM, DRU or FOA. For SECAF approved document, include a statement the same or substantially the same as the first sentence of this note.	

5.2. Participation in a SAP Directed by Another DoD Component or Agency. AF participation in another DoD component or agency's SAP, shall be documented in an MOA and approved by the AF SAPCO and the SPOC Executive Secretary, after coordination, at a minimum, with those with acquisition, contracting, fiscal, legal, manpower, operational, and security responsibilities. This also includes when organizations outside of the AF request an AF organization to accept funding and execute contracts to provide services, develop technology, etc. for their SAP. These MOAs must be updated or recertified, in writing, every five years.

5.3. Transfer of a SAP System Capability to/from Another DoD Component or Agency. An MOA shall be prepared by the PM and PSO for any SAP (also includes compartments, sub-compartment or projects) capability transferred to/from the Air Force from/to a non-Air Force organization in which the capability to be transferred requires continued resources to sustain (i.e. funding, manpower, etc.). The SECAF shall approve an MOA outlining the items in Table 7:

**Table 7. MOA Elements Required for a SAP System Capability Transfer**

Description of technology to be transferred (data/knowledge/equipment)
Gaining and losing organizations
Roles & responsibilities
Gaining CSA
Personnel security access requirements (if beyond standard requirements)
Logistics and sustainment requirements
Marking Guidelines and Instructions
Contracting Review
Legal Review
Resources necessary to sustain the program

## 6. The Appeal Board For SAP Access.

6.1. SAP Access Suspensions, Revocation and Reinstatements. The Security Director, AFOSI PJ, is authorized to suspend, revoke and reinstate SAP access. After review of the request to suspend access by the Security Director, AFOSI PJ, PSOs may suspend SAP access. In exigent circumstances, PSOs are empowered to suspend a person's access, but must immediately follow up with the Security Director, AFOSI PJ, for a final review. The

Director, AF SAPCO, is the approval authority to permit or continue access while any administrative inquiry or criminal investigation is being conducted.

6.2. PSAB Membership. The SAP PSAB consists of three voting members: Chair of the PSAB (The Director, AF SAPCO, permanent member) in his/her absence, the duties of Chair can be delegated to an individual at a minimum grade of O-5 or civilian equivalent. The second and third members will be selected by the PSAB Chair from a pool of candidates nominated by Secretariat offices. Individuals in this pool must be at minimum grade of O-5 or civilian equivalent and accessed to one or more SAPs. The Security Director and Deputy Director, AFOSI PJ, shall act as advisors to the PSAB. As determined by the PSAB Chair, non-voting members may participate in the PSAB. These members are typically subject matter experts required to provide advice to the Chair. A non-voting recorder shall be present to record all PSAB decisions.

6.3. Special Access Program Appeals. Each SAP accessed individual has the right to appeal any decision which limits or revokes their access to SAPs. The appeal process applies to all military, government employees, and contractor personnel supporting SAPs.

6.3.1. The SAP PSAB is the governing and decision authority for all SAP appeals.

6.3.2. This appeal process does not apply to SAP candidates who fail to meet the minimum SAP access eligibility requirements. These requirements include a current personnel security investigation, appropriate level of clearance, NTK or refusing to sign a SAP indoctrination agreement. These circumstances are not appealable by the SAP candidate.

6.3.3. Prospective board members shall disqualify themselves based on any conflict of interest such as a personal relationship with or prior knowledge of the appellant with respect to the disputed matters under consideration.

6.3.4. The PSAB Chair determines the hearing location within the Washington, DC area. A government employee's organization can authorize temporary duty assignment (TDY) funding for government appellants making a personal appearance. The government is not responsible for any expense incurred by an employee of a government contractor or any other non-government employee. Individuals are responsible for costs associated with their counsel.

6.3.5. The SAP accessed individual (appellant) must comply with the process reflected below:

6.3.5.1. Within 30 days of receiving the notification that their access was suspended or revoked, submit a request to the Director, AF SAPCO, explaining that they would like to exercise their right to appeal the decision.

6.3.5.2. The appellant can use the Appeal Board Review Format (Attachment 2) or an appropriate letter with the same information to request a review.

6.3.5.3. The appellant must indicate whether they shall appear in person at the PSAB hearing (If the appellant elects to appear personally, the appellant may be accompanied by one person serving as counsel to the appellant.) or; Request the PSAB review of all applicable records related to the decision and provides any additional mitigating documentation which was not previously provided.

6.3.6. PSAB process shall adhere to the requirements outlined below:

6.3.6.1. The PSAB shall notify the appellant, using Attachment 3 as a template, of the date and location of the hearing. The PSAB shall normally hear appeals within 60 days of receiving the appellant's request for a hearing.

6.3.6.2. The PSAB shall not call witnesses. The PSAB shall not request or conduct further investigation. The PSAB must render a decision based solely on the documents contained in the appeal package and information provided by the appellant.

6.3.6.3. Board members may ask the appellant appropriate questions.

6.3.6.4. Decisions shall be made by a majority vote.

6.3.6.5. The PSAB recorder shall tally the vote and prepare the reasons for the results.

6.3.6.6. The PSAB recorder shall send the appellant a letter reflecting the PSAB's decision and its reasons for upholding or reversing the decision to limit revoke the appellant's SAP access. An information copy of this correspondence shall be maintained in AFADS or its successor. All PSAB decisions are final.

## **7. Foreign Ownership, Control or Influence (FOCI).**

7.1. The following FOCI policy for U.S. companies subject to an FCL is intended to facilitate foreign investment by ensuring that foreign firms cannot undermine U.S. security and export controls to gain unauthorized access to critical technology, classified information, and special classes of classified information. A U.S. company is considered FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts. A national interest determination (NID) is the process the U.S. Government uses to make a determination on whether companies or firms operating under FOCI require access to classified information or performance of classified contracts.

7.2. A NID is a determination that release of the proscribed information to the company does not harm and is consistent with the national security interests of the United States. A NID is required when a company has FOCI and operates under an approved Special Security Agreement (SSA) as defined by the National Industrial Security Policy Operating Manual (NISPOM), and requires access to proscribed information. A company must have a current SSA prior to a NID determination approval. Before a FOCI firm participates on any contract activity with proscribed information, the FOCI must be mitigated by a NID or proxy agreement as outlined in the NISPOM.

7.3. To ensure timely and consistent handling of NID requests, the SECAF has identified SAF/AA as the senior official to coordinate compliance with current DoD policy and is the Air Force NID approval authority for SAP and collateral proscribed information. On behalf of SAF/AA, the Director or Deputy Director of SAF/AAZ shall also approve SAP and collateral NIDs. An approved NID must be in place prior to the FOCI firm being allowed

access to proscribed information. The Director of SAF/AAZ shall be responsible for forwarding the requests to the appropriate proscribed information owning agency for processing.

7.4. The GCA and the PSO determine if access to proscribed information is required to complete pre-contract award actions, perform on a new contract, or renew an existing contract. NIDs may be program-, project-, or contract-specific. For program and project NIDs, a separate NID is not required for each contract unless SAF/AAZ has determined otherwise. After receiving the required contractor documents, the GCA has 30 days to determine whether release of proscribed information is consistent with national security and the contract requirements. Within the 30 days, the request must be forwarded to the PEO and SAF/AAZ for approval. If the GCA requires additional time beyond 30 days, written notification from the requestor to SAF/AAZ must be provided. The PSO shall not upgrade an existing contractor clearance under an SSA to Top Secret unless an approved NID covering the prospective Top Secret access has been issued.

7.5. The GCA should coordinate with the PSO to prepare a NID request in accordance with the standard NID template in Attachment 4. The NID package should come with a Staff Summary Sheet with coordination from the GCA, the PEO and PSO. SAF/AAZ shall be listed as the approver in the Staff Summary Sheet. The cover letter from the GCA shall be used to discuss NID details and the tabs shall be used for required supporting documentation and shall indicate the date the request was received by the GCA. The package shall address:

7.5.1. What – specifically to what proscribed program or project does the contractor require access to?

7.5.2. Where – exact work location to include room numbers. Provide applicable DD Forms 254 for facility accreditation verification.

7.5.3. When – for what period of time is the NID requested? What is the period of performance for this contract?

7.5.4. Why - is it a sole-source contract? If so, what is the justification? If not sole source, why is it in the national security interest of the United States to grant a NID?

7.6. The NID request shall be processed within 30 days of the GCA receiving the contractor documentation. Where no interagency coordination is required, because the Air Force owns or controls all the proscribed information in question, the GCA in conjunction with the CSA, shall provide a final documented decision to the contractor within 30 days of the requested date for the NID. If the proscribed information is owned by, or under the control of, a department or agency outside of the Air Force (e.g. National Security Agency (NSA) for Communications Security, the Office of the Director of Intelligence (ODNI) for Sensitive Compartmented Information, and Department of Energy (DOE) for Restricted Data), the GCA shall have 60 days to provide a final documented decision from all applicable CSAs.

7.6.1. For existing acquisitions, where the program office or requiring activity has determined a NID is required, that office should contact SAF/AAZ for the course of action before issuing a stop work order, discontinuing payments or discontinuing obligating funds.

7.6.2. For new acquisitions, the contractor cannot have access to SAP information unless they have an approved NID for that program, project, or contract.

TIMOTHY A. BEYLAND  
Administrative Assistant

**(AFOTEC)**  
MATTHEW H. MOLLOY  
Major General, USAF

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

Information Security Oversight Office, Classified National Security Information, 32 CFR Part 2001 [Directive No. 1]

DoDD 5205.07, Special Access Program (SAP) Policy, 1 July 2010

DoDI 5205.11, Management, Administration, and Oversight of DoD Special Access Programs (SAPs), 6 February 2013

DoD 5240.1-R, Procedures for Governing the Activities of DoD Intelligence Components That Affect United States Persons, 7 December 1982

DoD AFMAN 33-302, Freedom of Information Act Program, 21 October 2010 (Incorporating Change 1 14 April 2012)

Directive-Type Memorandum (DTM) 09-019, Policy Guidance on Foreign Ownership, Control or Influence (FOCI), 2 September 2009 (Incorporating Change 1, 8 June 2010)

CJCSI 3120.08D, Integrated Joint Special Technical Operations, 28 January 2013

CJCSM 3150.29D, “Code Word, Nickname, and Exercise Terms Report (NICKA) System,” 15 October 2010

AFPD 16-2, Disclosure of Military Information to Foreign Governments and International Organizations, 10 September 1993

AFPD 16-6, International Arms Control and Nonproliferation Agreements, and the DoD Foreign Clearance Program, 29 December 2010

AFPD 16-7, Special Access Programs, 29 December 2010

AFPD 25-2, Support Agreements, 12 October 2012

AFPD 31-4, Information Security, 1 September 1998

AFPD 31-6, Industrial Security, 1 April 2000

AFPD 33-2, Information Assurance Program, 3 August 2011

AFPD 33-3, Information Management, 8 September 2011

AFPD 51-3, Civil Litigation, 21 May 1993

AFPD 61-3, Domestic Technology Transfer, 6 February 2001

AFPD 71-1, Criminal Investigations and Counterintelligence, 6 January 2010, (Incorporating Change 2, 30 September 2011)

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

AFI 10-601, Operational Capabilities Requirements Development, 12 July 2010.

AFI 16-603, Education and Training Requirements For Implementation of, and Compliance With, Arms Control Agreements, 9 June 2011

AFI 14-104, Oversight of Intelligence Activities, 23 April 2012.

AFI 14-111, Intelligence Support to the Acquisition Life-Cycle, 18 May 2012.

AFI 16-201, AF Foreign Disclosure and Technology Transfer Policy, 1 December 2004 (Incorporating Change 1, 11 August 2009)

AFI 16-501, Control and Documentation of Air Force Programs, 14 June 1994

AFI 16-601, Implementation of, and Compliance With, International Arms Control and Nonproliferation Agreements, 18 February 2011 (Incorporating Change 1, 15 November 2011)

AFI 16-604, Implementation of, and Compliance With, the Treaty On Open Skies, 28 March 2012

AFI 16-608, Implementation of, and Compliance with, the New Start Treaty, 18 January 2011

AFI 25-201, Support Agreements Procedures, 1 May 2005, (Incorporating Change 1, 28 January 2008 and certified current as of 1 July 2010)

AFI 31-101, Integrated Defense (FOUO), 8 October 2009

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

AFI 31-601, AFGM1, Industrial Security Program Management, 18 June 2012

AFI 51-303, Intellectual Property—Patents, Patent Related Matters, Trademarks and Copyrights, 1 September 1998

AFI 63-101, “Acquisition and Sustainment Life-Cycle Management, 3 April 2009 (Incorporating through Change 4, 3 August 2011)

AFI 61-301, The Domestic Technology Transfer Process and the Offices of Research and Technology Applications, 30 May 2001

AFI 63-602, Defense Production Act Title I--Defense Priorities and Allocations System, 18 December 2003

AFI 63-603, Defense Production Act Title III Program, 17 December 2003

AFI 65-201, Manager’s Internal Control Program Procedures, 20 January 2012

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

AFI 71-101, Volume 4, Counterintelligence, 8 November 2011

AFI 90-201, The Air Force Inspection System, 2 August 2013

AFI 90-301, Inspector General Complaint Resolution, 23 August 2011 (Incorporating Change 1, 6 June 2012)

AFI 99-103, Capabilities-Based Test and Evaluation, 26 February 2008 (Incorporating Change 2, 20 March 2009)

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

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

AFOSIMAN 71-144, Volume 1, Counterintelligence and Security Services,

***Adopted Forms***

AF Form 847, *Recommendation for Change of Publication.*

DD Form 254, *Contract Security Classification Specification*

***Abbreviations and Acronyms***

**AAA**—Access Approval Authority

**ACAT**—Acquisition Category

**AF**—Air Force

**AFAA**—Air Force Audit Agency

**AFADS**—Air Force Access Database System

**AFI**—Air Force Instruction

**AFROC**—Air Force Requirements Oversight Council

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

**AFOTEC**—Air Force Operational Test and Evaluation Center

**AFPD**—Air Force Policy Directive

**AMP**—Access Management Plan

**CA**—Cognizant Authority

**CAB**—Common Access Billet

**CASTS**—Configuration and Security Tracking System

**CI**—Counterintelligence

**CFIUS**—Committee on Foreign Investments in the United States

**CIO**—Chief Information Officer

**CISP**—Counterintelligence Support Plan

**CO**—Contracting Officer

**COCOMS**—Combatant Commands

**CPI**—Critical Program Information

**CSA**—Cognizant Security Authority

**CSAF**—Chief of Staff of the Air Force

**CC**—Critical Component

**CW**—Coal Warfighter

**DAA**—Designated Accreditation Authority

**DAB**—Defense Acquisition Board

**DCAA**—Defense Contract Audit Agency

**DCADS**—Distributed Common Access Database System  
**DCAPE**—Director, Cost Assessment and Program Evaluation  
**DCMA**—Defense Contractor Management Agency  
**DepSecDef**—Deputy Secretary of Defense  
**DIG**—Deputy Inspector General  
**DMAG**—Deputy’s Management Action Group  
**DNI**—Director of National Intelligence  
**DSS**—Defense Security Service  
**DoD**—Department of Defense  
**DOE**—Department of Energy  
**DRU**—Direct Reporting Unit  
**EA**—Executive Agent  
**FCL**—Facility Security Clearance  
**FM**—Financial Management  
**FOA**—Field Operating Agency  
**FOCI**—Foreign Ownership, Control and Influence  
**FOIA**—Freedom Of Information Act  
**GCA**—General Contracting Authority  
**GSSO**—Government SAP Security Officer  
**IA**—Information Assurance  
**IAW**—in accordance with  
**ICD**—Initial Capabilities Document  
**IG**—Inspector General  
**IIA**—Independent Intelligence Assessments  
**IJSTO**—Integrated Joint Special Technical Operations  
**IOC**—Initial Operating Capability  
**IS**—Information System  
**ISR**—Intelligence, Surveillance and Reconnaissance  
**ISSO**—Information System Security Officer  
**JCIDS**—Joint Capabilities Integration Development System  
**JROC**—Joint Requirements Oversight Council  
**MAJCOM**—Major Command

**MDAP**—Major Defense Acquisition Program  
**MOA**—Memorandum of Agreement  
**MOU**—Memorandum of Understanding  
**NICKA**—Code Word, Nickname, and Exercise Term  
**NID**—National Interest Determination  
**NISP**—National Industrial Security Program  
**NISPOM**—National Industrial Security Program Operating Manual  
**NTK**—Need To Know  
**NSS**—National Security System  
**OA**—Oversight Authority  
**OCA**—Original Classification Authority  
**ORTA**—Office of Research and Technology Application  
**OPSEC**—Operations Security  
**OSD**—Office of the Secretary of Defense  
**OTA**—Operational Test Agency  
**OT&E**—Operational Test and Evaluation  
**PEM**—Program Element Monitor  
**PEO**—Program Executive Officer  
**PB**—President’s Budget  
**PBR**—Program and Budget Review  
**PID**—Program Identifier  
**PM**—Program Management  
**POM**—Program Objective Memorandum  
**PPBE**—Planning, Programming, Budgeting and Execution  
**PPP**—Program Protection Plan  
**PSAB**—Personnel Security Appeal Board  
**PSAP**—Prospective Special Access Program  
**PSO**—Program Security Officer  
**QDR**—Quadrennial Defense Review  
**RAP**—Review and Approval Process  
**RDS**—Records Disposition Schedule  
**SAB**—Scientific Advisory Board

**SAP**—Special Access Program  
**SAPCO**—Special Access Program Central Office  
**SAPD**—Special Access Program Directive  
**SAPF**—Special Access Program Facility  
**SAPOC**—Special Access Program Oversight Committee  
**SCG**—Security Classification Guide  
**SCI**—Sensitive Compartmented Information  
**SCIF**—Sensitive Compartmented Information Facility  
**SECAF**—Secretary of the Air Force  
**SecDef**—Secretary of Defense  
**SETA**—Security Education, Training and Awareness  
**SORB**—SAP Oversight Review Board  
**SPeD**—Security Professional Education Development  
**SPOC**—Special Programs Oversight Committee  
**SPRG**—Special Programs Review Group  
**SRG**—Senior Review Group  
**SSA**—Special Security Agreement  
**SSE**—Systems Security Engineering  
**SSWG**—SAP Senior Working Group  
**SME**—Subject Matter Expert  
**TIG**—The Inspector General  
**U.S.C.**—United States Code

### *Terms*

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

**Apportioned SAP**— A SAP that is formally included in the IJSTO process for combatant command use during deliberate planning, crisis action response, and operational employment.

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

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

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

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

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

**Cover**— The concealment of true identity, purpose, or organizational affiliation with assertions of false information as part or, or in support of, official duties to carry out authorized activities and lawful operations.

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

**Critical Components**— CCs are those resources, which if unavailable or compromised, could seriously impact development, production, delivery, or operation of a system, component, or technology.

**Designated Accreditation Authority (DAA)**— A designated official with the authority to formally assume responsibility for operating a SAP IS at acceptable level of risk.

**Government SAP Security Officer (GSSO)**— The GSSO is a government employee, appointed in writing and assigned to provide SAP security administration and management within their respective HAF office, MAJCOM, subordinate command, or similar office. GSSOs act as the security focal point, working in tandem with the PSO, to create a secure environment to facilitate the successful development and execution of SAPs at their location. Contractor personnel may support GSSO functions only to the extent that they are subject to the direction of specified government personnel who perform all discretionary GSSO functions on behalf of the United States Government. Use of contractor personnel to act as a GSSO may only occur with the approval of the Director, AF SAPCO. This approval shall be annually validated.

**Information System Security Officer (ISSO)**— Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

**Intra-governmental Support**— Support provided by a DoD activity to a non-DoD Federal activity and vice versa -- does not include support provided to or received from foreign governments.

**Inter-service Support**— Support provided by one DoD activity to a DoD activity of another Military Service, Defense Agency, Unified Combatant Command, Army Reserves, Navy Reserves, Air Force Reserves, Marine Corps Reserves, Air National Guard, or Field Activity.

**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.

**Memorandum of Understanding (MOU)**— Written agreements between programs that do not obligate SAP resources. MOUs shall be executed when it is necessary to exchange SAP information between services. MOUs define general areas of understanding between two or more parties -- explains what each party plans to do; however, what each party does is not dependent on what the other party does (e.g., does not require reimbursement or other support from receiver). MOUs must be updated or recertified, in writing, every five years.

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

**Office of Research and Technology Applications (ORTA)**— Office required by 15 U.S.C. § 3710(b) to oversee the Domestic Technology Transfer Program at a laboratory and/or technical activity. Normally, an ORTA comprises individuals with expertise in marketing, public relations, intellectual property, patent law, and scientific and technical information.

**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 (OA)**— The 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.

**Privileged User**— An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions.

**Program Identifier (PID)**— An unclassified abbreviation for an assigned SAP, compartment, sub-compartment or project nickname or code word. PID letters shall be drawn from the letters within the nickname or code word.

**Program Security Officer (PSO)**— The PSO is a government employee assigned to AFOSI PJ who is responsible for executing SAP security responsibilities for a specific SAP, compartment, sub-compartment, project and/or geographical region/MAJCOM. Contractor personnel may support PSO functions managed by AFOSI PJ only to the extent that they are subject to the direction of specified AFOSI PJ personnel who perform all discretionary PSO functions on behalf of the United States Government. Use of contractor personnel to act as a PSO may only occur with the approval of the Director, AF SAPCO. This approval shall be annually validated.

**Program Termination**— A SAP, compartment, sub-compartment, or project activities have ceased and shall not be restarted. SAP enhanced security protective measures are still required.

**Program Disestablishment**— Action taken when enhanced security protective measures are no longer required for the information contained within the program. This action may include termination, cancelation, or transition of a SAP.

**Program Transition**— An action that results in a change in protection level for the SAP material such SAP to non-SAP, classified to unclassified, or the transfer of information to another SAP or compartment.

**Proscribed Information**— Information defined as COMSEC, SCI, Restricted Data, Formally Restricted Data, SAP, or Top Secret. The following are the approved CSAs for proscribed information: National Security Agency (NSA) for COMSEC, Director of National Intelligence (DNI) for SCI, Department of Energy (DOE) for RD and FRD, DoD Component Head for SAP, the Military Departments for their TOP SECRET information, and other Executive Branch Departments and Agencies for classified information under their cognizance.

**Prospective SAP**— An AF program or activity for which enhanced security measures have been proposed and approved to facilitate security protections prior to establishing the effort as a SAP.

**Revocation of SAP Access**— A decision to take away SAP access.

**Special Access Program**— An activity which has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within a SAP is identified by an SCG.

**SAP Compartment**— An effort under a SAP, approved by the AF SAPCO, and protected by a separate SCG or based upon written guidance derived from the existing SCG of its umbrella. A person accessed to a compartment is accessed to all sub-compartments and projects below the compartment, unless an exception is specifically approved by the AF SAPCO.

**SAP Project**— A narrowly-focused, short-term effort under a SAP sub-compartment approved by the AF SAPCO that is protected by a specific SCG or based upon written guidance derived from existing SCG of its parent sub-compartment. Each project shall be assigned a nickname, PID, and code word, if applicable.

**SAP Sub-compartment**— An effort under a SAP compartment approved by the AF SAPCO and protected by a distinct and separate designated SCG or based upon written guidance derived from an existing SCG of its SAP compartment. A person accessed to a sub-compartment is accessed to all projects below the sub-compartment, unless an exception is specifically approved by the AF SAPCO.

**Suspension of SAP Access**— A temporary action to put on hold an individual's SAP access by an appropriate authority. SAP access cannot be reinstated until a full review of the details causing the suspension is completed.

**Unacknowledged SAP**— A SAP having enhanced security protection measures ensuring the existence of the program is not acknowledged, affirmed, or made known to any person not authorized for such information.

**Waived SAP**— A SAP for which the SecDef has waived applicable reporting in accordance with IAW Title 10 U.S.C. Section 119 following a determination of adverse effect to national security. An unacknowledged SAP that has more restrictive reporting and access controls than other unacknowledged SAPs.

## Attachment 2

## INSTRUCTIONS FOR APPEAL BOARD APPEARANCES (REQUEST FORMAT EXAMPLE)

Figure A2.1. Instructions for Appeal Board Appearances (Request Format Example)

**REQUEST**FROM: *(Insert your name and mailing address)*\_\_\_\_\_  
\_\_\_\_\_

SUBJECT: Request for Appeal Board Review

I request a Secretary of the Air Force Special Access Program Personnel Security Appeal Board (SAP PSAB) review of the decision to limit or revoke my access to Special Access Programs.

I request *(check a or b)*:

a) The SAP PSAB to review the appeal package (You may attach additional mitigating documentation; I shall not make a personal appearance--See Note.)

b) To make a personal appearance before the SAP PSAB

If b is checked, check either (1) or (2)

1) I plan to have counsel (at my own expense) appear with me at the SAP PSAB.

2) I do not plan to have counsel appear with me.

NOTE: The Adjudicative Reviewer shall forward your case file and any other documentation you or other agencies/personnel have provided previously to the Board. You do not need to send duplicate copies.

If you plan to appear personally, please provide the following information so that you may be contacted by an Adjudicator who shall provide the date, time and exact location of the SAP PSAB meeting.

Work Phone: \_\_\_\_\_

Home Phone: \_\_\_\_\_

This notice must be returned no later than \_\_\_\_\_ to the contact information reflected on the letter revoking your access:

\_\_\_\_\_

## Attachment 3

## INSTRUCTIONS FOR APPEAL BOARD APPEARANCES (RESPONSE FORMAT EXAMPLE)

Figure A3.1. Instructions for Appeal Board Appearances (Response Format Example)

**FROM:** (Name and Address of Advising Activity)

**SUBJECT:** Instructions for Appeal Board Appearance

**TO:** (Name and Address of Appellant)

1. You indicated that you wanted to appear personally before the Special Access Program Personnel Security Appeal Board.

2. The SAP PSAB has scheduled your appeal as follows:

Date \_\_\_\_\_ Time \_\_\_\_\_

Location \_\_\_\_\_

3. Should this time be inconvenient, please call \_\_\_\_\_ at \_\_\_\_\_ to provide the reason(s) for delay and rescheduling information. Postponement of the appearance can be granted only for justified reason(s).

4. The appellant may:

a. Be represented by one counsel or personal representative at his/her own expense

b. Make an oral presentation not to exceed two hours

c. Submit additional relevant documents not already provided to the Appeal Board

5. The appellant may not:

a. Call witnesses

b. Question the Board concerning the substance of the appeal

6. Travel costs for the government appellants are at the discretion of the government organization. The government is not liable for any cost borne by the contractor appellant.

7. Appeal Board members shall have reviewed your case file. Therefore, we suggest you use your allotted time to clarify your reasons for overturning the denial or suspension or providing additional information. We recommend you not repeat material contained in your file or in documents you previously provided. At the end of the personal appearance, you may make a closing statement.

8. For further information concerning Appeal Board protocol, contact

\_\_\_\_\_ at \_\_\_\_\_.

SIGNATURE BLOCK

Secretary

Special Access Program Appeal Board

## Attachment 4

## SAMPLE – NATIONAL INTEREST DETERMINATION (NID) REQUEST PACKAGE

## Sample – National Interest Determination (NID) Request Package

MEMORANDUM FOR ASSISTANT SECRETARY OF THE AIR FORCE

FROM: FULL NAME / IDENTIFICATION OF REQUESTING GOVERNMENT  
CONTRACTING AUTHORITY (GCA)

SUBJECT: Request for Consideration of National Interest Determination (NID) (FOUO)

References: "National Industrial Security Program Operating Manual" (NISPOM) (DoD 5220.22-M, para 2-309) and Executive Order 12829, "National Industrial Security Program" (NISP)

1. Pursuant to the above references, request favorable consideration of the \_\_\_\_\_ in granting a National Interest Determination (NID) to FULL NAME / IDENTIFICATION AND ADDRESS OF COMPANY (*complete identification to include all subcontractors, subsidiaries, partnerships, and full description of relationships/individual product lines, etc. shall be detailed in Tab "A" as outlined below*).
2. The following justification and supporting data is provided for your review and consideration:
  - a. We request favorable consideration be given SPECIFIC PROGRAM/PROJECT NAME/LEVEL OF DETAIL (*detail specific "proscribed information" to include specific levels, etc.*). In the enclosed attachments our request shall detail compelling evidence that release of such information to INSERT NAME OF COMPANY advances the national security interests of the United States. The attachments are as follows:
    - (1) Tab "A": *Staff Summary Sheet – HQ XXXX Coordination with cognizant PM, cognizant CO, cognizant PEO, XXXXXXXXXX, XXXXXXXXXX, XXXXXXXXXX, SAF/GC; Approval SAF/AA.*
    - (2) Tab "B": *Identification of the proposed awardees along with a synopsis of its foreign ownership (include solicitation and other reference numbers to identify the action).*
    - (3) Tab "C": *General description of the procurement and performance requirements.*
    - (4) Tab "D": *Identification of national security interests involved and the ways in which award of the contract helps advance those interests.*
    - (5) Tab "E": *A description of any alternate means available to satisfy the requirement, and the reasons alternative means are not acceptable.*
    - (6) Tab "F": *Government's Counterintelligence Assessment/Foreign Ownership Issues.*

(7) Tab "G": *Proposed NID Approval / Disapproval Letter (XXXXX)*

***Processing Note:*** *All requests for NIDs shall be initiated by the GCA. A company may assist in the preparation of an NID, but the GCA is not obligated to pursue the matter further unless it believes further consideration to be warranted. The GCA shall, if it is supportive of the NID, forward the case through appropriate agency channels to the ultimate approval authority within that agency. If the proscribed information is under the classification or control jurisdiction of another agency, the approval of the cognizant agency is required; e.g., NSA for COMSEC, DCI for SCI, DOE for RD and FRD, the Military Departments for their TOP SECRET information, and other Executive Branch Departments and Agencies for classified information under their cognizance. It is the responsibility of the cognizant approval authority to ensure that pertinent security, counterintelligence, and acquisition interests are thoroughly examined. Agency-specific case processing details and the senior official(s) responsible for rendering final approval of NID's shall be contained in the implementing regulations of the U.S. agency whose contract is involved.*

3. The designated point of contact for all matters related to this specific NID request may be directed to the undersigned. You may contact me via unclassified email at: [ira.sample@emailaddress.com](mailto:ira.sample@emailaddress.com) or telephone (xxx-xxx-xxxx).

IRA M. SAMPLE  
Government Contracting Authority (GCA)

Attachments:

- 1.Tab A (Staff Summary Sheet – HQ AF Coordination with cognizant PM, cognizant CO, cognizant PEO, GC; Approval by SAF/AA)
- 2.Tab B (Full company identification & foreign ownership synopsis)
- 3.Tab C (Procurement and performance requirements)
- 4.Tab D (Rationale for advancement of National Security interests)
- 5.Tab E (Alternative means of satisfying requirements)
- 6.Tab F (Counterintelligence Assessment/Foreign Ownership Issues)
- 7.Tab G (Proposed NID Approval/Disapproval Letter)

**Tab A**

*(Staff Summary Sheet – HQ XXXX Coordination with cognizant PM, cognizant CO, cognizant PEO and approval by SAF/AA)*

**Tab B**

*(Full company identification & foreign ownership synopsis)*

1. Full Company Identification:

a. Company Name: \_\_\_\_\_

b. FSC/Cage Code: \_\_\_\_\_

c. Facility Clearance: \_\_\_\_\_

d. Physical Location (Street Address): \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

e. Is Corporate Headquarters same as Item "d" above: Yes \_\_\_ No \_\_\_

(1) If "No" - specify / list Corporate Headquarters information (Items "a" - "d" above).

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

f. Facility Clearance: \_\_\_\_\_

g. Product Line (relevant to this request; detail by location/activity and by subsidiary/subcontractor relationship, etc.): \_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

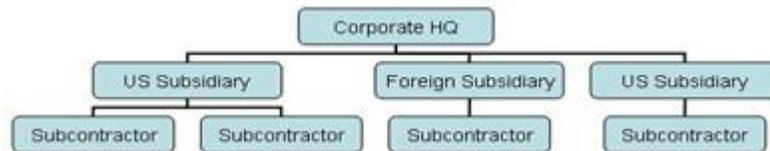
\_\_\_\_\_

h. Foreign Ownership Synopsis & Corporate Relationships: (detail all foreign ownership, partnerships, subsidiaries, affiliations - in addition to narrative; provide a linear organizational chart depicting all corporate entities/relationships, etc.)

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_



i. Detail all previously granted and current Special Security Agreements, Security Control Agreements, Voting Trust Agreements and Proxy Agreements and/or other relevant National Interest Determinations:

---

---

---

*(Note: All question/answer spaces above are not representative of allowable narrative - continue on additional pages to sufficiently detail)*

**Tab C**

*(Procurement and performance requirements)*

**Tab D**

*(Rationale for advancement of National Security interests – **Note:** The following statement, "Release of the proscribed information to the company shall not harm the national security interests of the United States." must be included)*

**Tab E**

*(Alternative means of satisfying requirements)*

**Tab F**

*(CI Assessment/Foreign Ownership Issues — **Note:** To be completed by cognizant CI service activity and forwarded to the GCA for inclusion in the NID Request package)*

**Tab G**

*(Proposed NID Approval / Disapproval Letter (XXXXX))*