DEPARTMENT OF THE AIR FORCE
HEADQUARTERS AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

AFI16-701_AFMCSUP_AFMCGM2025-01
23 July 2025

MEMORANDUM FOR ALL AFMC SPECIAL ACCESS PROGRAM (SAP) UNITS

FROM: AFMC/CC
4375 Chidlaw Road, Room A-135
Wright-Patterson AFB OH 45433-5006

SUBJECT: Air Force Materiel Command (AFMC) Guidance Memorandum to Air Force Instruction (AFI) 16-701, *Management, Administration and Oversight of Special Access Programs.*

RELEASABILITY: There are no releasability restrictions on this publication

By order of the Commander, Air Force Materiel Command (AFMC), this Guidance Memorandum (GM) immediately implements guidance for a to be published AFMC supplement to Air Force Instruction (AFI) 16-701, *Management, Administration and Oversight of Special Access Programs.* Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other AFMC publications, the information herein prevails, in accordance with Department of the Air Force (DAFI) 90-160, *Publications and Forms Management* and Department of the Air Force Manual 90-161, *Publishing Processes and Procedures.*

This Guidance Memorandum implements supplemental guidance for the purpose of establishing roles and responsibilities with AFMC for the management, administration, oversight, and support of AFMC SAP Activities across the Command.

This publication applies to all AFMC Regular Air Force. This publication does not apply to United States Space Force, Air Force Reserve, or Air National Guard units. Ensure all records generated as a result of processes prescribed in this publication adhere to AFI 33-322, *Records Management and Information Governance Program,* and are disposed of in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System.

This Memorandum becomes void after one year has elapsed from the date of this Memorandum, or upon publication of a new publication permanently establishing this guidance whichever is earlier.

LINDA S. HURRY
Lieutenant General, USAF
Commander

Attachment:
1. AFMC Interim Guidance to AFI 16-701

Attachment 1

AFMC Interim Guidance to AFI 16-701, *Management, Administration and Oversight of Special Access Programs*

This GM supports the protection of AFMC critical missions, developing, fielding, and sustaining war-winning expeditionary capabilities within Special Access Programs (SAPs) by establishing an organizational support structure for the management, administration, oversight, and support of SAPs across the Command. The authorities to waive wing/unit level requirements in this GM are identified with a Tier ("T-0, T-2, T-3") number following each compliance statement. See Department of the Air Force Manual (DAFMAN) 90-161, *Publishing Processes and Procedures,* for a description of the authorities associated with the Tier designators. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to this GM's OPR for non-tiered compliance items, as applicable.

2.25. (Added-AFMC) HQ AFMC Special Access Program Management Office (SAPMO) Director shall:

2.25.1. **(Added-AFMC) Serve** as the HQ AFMC Commander's single organizational focal point within HQ AFMC for policy, management, security, coordination, dissemination, and reporting of AFMC SAP activities, herein referred to as AFMC Special Access Program Management Office (SAPMO) and led by the Commander's appointed Director.

2.25.2. **(Added-AFMC)** Serve as a conduit and facilitate AFMC corporate review process of SAP activities, in a parallel yet separate and distinct order, to provide appropriate security in accordance with Air Force Policy Directive (AFPD) 16-7, *Special Access Programs* and AFMC Instruction (AFMCI) 90-601, *AMFC Corporate Structure.*

2.25.3. **(Added-AFMC)** Support AFMC SAP activities through execution of mission per AFMC Mission Directive (AFMCMD) 401, *Headquarters Air Force Materiel Command*

2.25.4. **(Added-AFMC)** Shape, integrate, implement, and manage policies and procedures to aid in the secure management, administration, and oversight of Command SAP activities, including the protection of SAP Information Technology (IT).

2.25.5. **(Added-AFMC)** Ensure a Command Government SAP Security Officer (GSSO) is appointed in writing to serve as the SAP Security policy, oversight, and compliance lead.

2.25.6. **(Added-AFMC)** Appoint in writing a qualified Command Information Systems Security Manager (ISSM) to support AFMC subordinate unit ISSMs, SAP IT Authorizing Officials, DAF Enterprise IT initiatives, to serve as the focal point for DAF Chief Information Officer (CIO) reporting requirements, and to serve as the primary Cybersecurity policy advisor for AFMC MAJCOM personnel on all matters involving the security of SAP information systems under the purview of AFMC.

2.25.7. **(Added-AFMC)** Support the Command Inspector General (IG) Program in accordance with DAFI 90-302, *The Inspection System of the Department of the Air Force* and Department of Defense Manual (DoDM) 5205.07, *DoD Special Access Program Security Manual.*

2.26. (Added-AFMC) Command GSSO shall:

2.26.1. **(Added-AFMC)** Support the responsibilities outlined in para 2.25., as a key member of the AFMC SAPMO staff.

2.26.2. **(Added-AFMC)** Establish and serve as a conduit for Command SAP activities and security professional to seek clarity and guidance on SAP policies and procedures; disseminate and track Enterprise Task Management Software Solution (ETMS2) tasks related to SAP security; identify Center and/or enterprise security issues for advocacy to HQ AFMC and/or Headquarters Air Force (HAF), etc.

2.26.3. **(Added-AFMC)** Appoint a Command SAP Security Compliance Inspection Lead (SSCIL) to manage and provide oversight of the Command SAP Security Compliance Inspection (SSCI) program.

2.26.4. **(Added-AFMC)** Supplement the SSCI process in order to clearly define and assess the roles and responsibilities of AFMC oversight activities (i.e., Center Special Program Office (CSPO)); implement supplemental compliance checklists to assess compliance with AFMC policies. Prior to implementation, coordinate supplemental process with SSCI inspectors and GSSOs.

2.26.5. **(Added-AFMC)** Coordinate and consolidate SSCIs to the maximum extent possible with overarching SAP IG inspections, as determined by AFMC/IG in coordination with the AFMC Command SSCIL.

2.26.6. **(Added-AFMC)** Establish and maintain a Command Organize, Train, and Equip (OT&E) Security Education Training and Awareness (SETA) program to enhance AFMC SAP Security posture and culture.

2.26.7. **(Added-AFMC)** Establish a system to collect, maintain, and report metrics on Command SAP security incidents and compliance inspection deficiencies to identify and report trends to HQ AFMC Senior Leaders to identify necessary changes to SAP SETA programs and policy.

2.26.8. **(Added-AFMC)** Establish and maintain an AFMC SAP Facilities Oversight Listing (SAPFOL) identifying all AFMC SAP Facility (SAPF) accreditations and assign a unique SAPF identification. Adjust and update data collection requirements identified in the SAPFOL as necessary.

2.26.9. **(Added-AFMC)** Ensure Command SAP Personnel Security Officials (SPOs) are trained and appointed to support program access in accordance with approved DAF SPO Training and Certification process.

2.27. (Added-AFMC) Command ISSM shall:

2.27.1. **(Added-AFMC)** Support the responsibilities outlined in para 2.25, as a key member of the AFMC SAPMO staff.

2.27.2. **(Added-AFMC)** Establish and serve as a conduit for Command SAP activities and Cybersecurity professionals to seek clarity and guidance on SAP policies and procedures; support the identification and report of SAP information systems.

2.27.3. **(Added-AFMC)** In coordination with the Command SSCIL, support SAP Security Compliance Inspections through the execution of the Cybersecurity Risk Management Framework (RMF) checklist.

2.27.4. **(Added-AFMC)** In coordination with the Command GSSO, establish and maintain a Cyber SETA program to enhance AFMC SAP Security posture and culture. Support the Command SAP SETA program to shape and develop Cybersecurity workforce products and initiatives.

2.27.5. **(Added-AFMC)** Establish documented processes to collect, maintain, and report metrics to the Command GSSO on Command SAP cyber incidents and compliance inspection deficiencies to identify trends and recommendations to affect changes to SAP SETA programs and policy.

2.27.6. **(Added-AFMC)** Establish a system to collect, maintain, and report on AFMC SAP information systems as required by the DAF Special Access Program Central Office (SAPCO) or DAF CIO.

2.27.7. **(Added-AFMC)** Establish a system to collect, maintain, and report all Command SAP IT Privileged Account Holders to DAF SAPCO and/or AFOSI PJ when requested and include as a minimum the following information:

2.27.7.1. **(Added-AFMC)** Name/Grade

2.27.7.2. **(Added-AFMC)** Duty Title

2.27.7.3. **(Added-AFMC)** Organization

2.27.7.4. **(Added-AFMC)** Position (i.e., Contractor, ISSM, Information System Security Officer (ISSO), IT, etc)

2.27.7.5. **(Added-AFMC)** Certification Information

2.28. (Added-AFMC) Command SSCIL shall:

2.28.1. **(Added-AFMC)** In coordination with the AFMC Command GSSO, appoint Center inspectors to conduct SSCIs on behalf of AFMC SAPMO.

2.28.2. **(Added-AFMC)** Establish, execute, and oversee the implementation of a robust Command SSCI program ensuring SSCIs are conducted as required and deficiencies are tracked from cradle-to-grave.

2.28.3. **(Added-AFMC)** Develop and disseminate training and certifications, guidance, procedures, and processes relating to conducting SSCIs and support the overall Command sight picture for SAP security health.

2.28.4. **(Added-AFMC)** Maintain a record of certified inspectors and most recent training completion date.

2.28.5. **(Added-AFMC)** In collaboration with each AFMC Center, develop a joint-inspection planning schedule and provide it to AFMC IG.

2.28.6. **(Added-AFMC)** Ensure Command and Center Inspection Team members are trained and aware of their responsibilities in accordance with DoD, AF, and AFMC policy to include this GM prior to conducting inspections.

2.28.7. **(Added-AFMC)** Coordinate with each Center's primary SSCI Inspector for inspections and re-inspections to validate ratings and findings. Once validated, report the inspection results to the AFMC/IG, AFMC Command GSSO, SAPMO Director, and DAF SAPCO within two working days.

2.28.8. **(Added-AFMC)** Ensure final inspection reports and corrective action plans (CAPs) are produced as key artifacts for deficiency management.

2.28.9. **(Added-AFMC)** Develop standardized reporting process and documentation for recording and reporting the details and actions taken or to be taken to close out SSCI findings. All CAPs must be endorsed by organizational leadership and the PSO.

2.28.10. **(Added-AFMC)** In coordination with the AFMC Information Security Action Officer, produce annual compliance trends and analysis report to identify potential policy gaps and training improvement opportunities.

2.29. (Added-AFMC) HQ AFMC Center Commanders shall:

2.29.1. **(Added-AFMC)** Establish a CSPO to support Center SAP activities, as applicable; serve as the organizational focal point for SAP activities; and, by extension, support the mission and responsibilities of the AFMC SAPMO in the management, administration, and oversight of subordinate SAP activities.

2.29.2. **(Added-AFMC)** Ensure CSPO staff are provided direct access and streamlined communications to the Center Commander, subordinate SAP activities, AFMC SAPMO, and other SAP activities as required. The CSPO, at a minimum, will consist of the following positions:

2.29.2. **(Added-AFMC)** An Assistant to the Commander for Special Programs (ACSP), appointed in writing, to serve as the CSPO Lead.

2.29.2.2. **(Added-AFMC)** A Center GSSO.

2.29.2.3. **(Added-AFMC)** A Center ISSM.

2.29.3. **(Added-AFMC)** Ensure the Center GSSO is appointed as an Organizational Senior Functional (OSF) for the Center SAP security workforce and is delegated responsibilities, in coordination with Center Senior Functional (CSF), for the oversight of Center SAP personnel actions including manpower position allocations, classification, hiring, moving, and workforce professional development.

2.30. (Added-AFMC) Assistant to the Commander for Special Programs shall:

2.30.1. **(Added-AFMC)** Lead the CSPO as the single focal point for coordination, dissemination, and reporting of Center SAP activities and serve as the liaison between the AFMC SAPMO and the respective Center Commander and subordinate SAP units.

2.30.2. **(Added-AFMC)** Serve as the Center Commander's SAP technical subject matter expert (SME) and principal advisor for SAP insight and awareness.

2.30.3. **(Added-AFMC)** Ensure respective Program Executive Offices (PEOs), Directorates, and Units have and maintain appropriate SAP accesses in order to execute the organization's mission in support of each Center Commander.

2.30.4. **(Added-AFMC)** Function as a Center focal point for planning, programs, and Center requirements (e.g. Infrastructure, facilities, SAP IT); Center-level SAP policy, guidance, and supplements, as applicable; and Center SAP processes and improvements.

2.30.5. **(Added-AFMC)** Function as a Center focal point for all AFMC SAP taskings/suspense, to include but not limited to coordination of Program Objective Memorandum (POM) inputs, unfunded requirements, and annual AFMC SAP award packages; coordination with AFMC IG for SSCILs; and other formal DoD, AF, and AFMC tasks.

2.30.6. **(Added-AFMC)** Function as a Center focal point for AFMC/IG and the Command SSCIL in support of SSCIs, to include but not limited to inspection schedule coordination and identifying the responsible SAP-accessed functional with pertinent oversight authority.

2.30.7. **(Added-AFMC)** Submit requests to the AFMC Command SSCIL for SSCI Inspector Appointment.

2.30.8. **(Added-AFMC)** Coordinate all requests for AFMC participation in support of non-AFMC SAP activities through command channels (i.e. ACSP through the AFMC SAPMO Director to DAF SAPCO).

2.30.9. **(Added-AFMC)** Provide oversight for the appropriate staffing, monitoring, and submission of SAP security documentation subject to AFMC SAPMO oversight, approval, or coordination (e.g. Access Approval Authority (AAA) delegation and training; Access Management Plan (AMP) change requests, billet request, or development; and Program Access Requests (PARs), as necessary)).

2.30.10. **(Added-AFMC)** Appoint in writing an appropriately trained individual to serve as the Center GSSO.

2.30.11. **(Added-AFMC)** Appoint in writing appropriately qualified individual to serve as the Center ISSM.

2.31. (Added-AFMC) AFMC Center GSSO shall:

2.31.1. **(Added-AFMC)** Support the ACSP in the responsibilities outline in para 2.30, as a key member of the CSPO staff.

2.31.2. **(Added-AFMC)** Execute SSCIs on Center SAP activities on behalf of AFMC SAPMO, in coordination with and direction from the Command SSCIL and Command GSSO, to assess compliance of Center SAP activities in accordance with applicable DoD, AF, and AFMC policies.

2.31.3. **(Added-AFMC)** In coordination with the AFMC SAPMO, serve as a Center SAP Security policy SME and conduit for Center SAP activities and security professionals to seek clarity and guidance on SAP policies and procedures; support the identification of policy issues and gaps; advocate for policy change recommendations, training, and inspection criteria; and disseminate and track SAP security tasks as required.

2.31.4. **(Added-AFMC)** Shape, implement, and disseminate SAP security policy, guidance, and procedures to aid in the protection of Center SAP activities and support the Command SAP SETA program.

2.31.5. **(Added-AFMC)** Collect Center SAP activities' security incident metrics and report to the Command GSSO, or designee, on a monthly basis, no later than the 15th of each month. Immediately notify the Command GSSO of any incident that results in senior leader or Wing/Complex-level leadership involvement.

2.31.6. **(Added-AFMC)** Appropriately staff, monitor, and submit SAP security documentation subject to AFMC SAPMO oversight, approval, or coordination as applicable (e.g. AAA delegation and training; AMP change requests and billet requests, and PARs).

2.31.7. **(Added-AFMC)** Ensure SPOs are properly trained and appointed in writing by the appropriate authority to support Center personnel with necessary program accesses applicable to mission execution.

2.31.8. **(Added-AFMC)** Update and maintain the AFMC SAPFOL for Center SAP activities on a monthly basis, no later than the 15th of each month, in coordination with the AFMC SAPMO. Request a unique SAPF accreditation AFMC identifier upon the appointment of a Site Security Manager for all SAPF new construction and all modifications not assigned an AFMC identifier.

2.31.9. **(Added-AFMC)** Establish and maintain situational awareness of subordinate activity GSSO staffing issues. Report to the Command GSSO any potentially negative impacts on SAP Security management resulting from staffing issues.

2.31.10. **(Added-AFMC)** Maintain Center and Unit distribution lists to ensure effective dissemination of SAP policy, guidance, tasks, and awareness messages.

2.31.11. **(Added-AFMC)** Submit requests to the Command SSCIL for SSCI Inspector appointment.

2.31.12. **(Added-AFMC)** Conduct site visits on new SAP activities within 12 months of establishment to review security management operations to ensure compliance with current DoD, DAF, and AFMC policies. Document the details of all site visits and provide a completed report to the Command GSSO for review/awareness. Center SAP activities may request a formal Staff Assistance Visit (SAV) in lieu of a site visit. All documentation will be submitted to the AFMC IG through the Command SSCIL as required.

2.31.13. **(Added-AFMC)** Oversee Center SAP security personnel actions as the designated OSF for SAP.

2.32. (Added-AFMC) AFMC Center ISSM shall:

2.32.1. **(Added-AFMC)** Support the ACSP in the responsibilities outlined in para 2.30, as a key member of the CSPO staff.

2.32.2. **(Added-AFMC)** Serve as a SAP Cybersecurity SME and be a liaison/information conduit for Cybersecurity related policy, tasks, issues, etc., between Center SAP activities, the AFMC SAPMO, Command ISSM, and the respective Center ACSP.

2.32.3. **(Added-AFMC)** Execute the reporting of DAF CIO reporting requirements for SAP IT systems for which they are responsible in accordance with AFI 17-101, *Risk Management Framework for AF Information Technology.*

2.32.4. **(Added-AFMC)** Execute cyber orders as defined by AFI 17-201, *Command and Control (C2) for Cyberspace Operations,* which apply to SAP IT systems. When cyber order reporting is required, the CSPO will coordinate with SAP activities to submit consolidated reports to the AFMC SAPMO.

2.32.5. **(Added-AFMC)** Execute SAP Cybersecurity RMF compliance inspections of Center SAP activities, assessing information systems, networks, and components for proper configuration and authorization to operate within AFMC SAP accredited areas.

2.32.6. **(Added-AFMC)** Report all cybersecurity related incidents to the Center GSSO and Command ISSM.

2.32.7. **(Added-AFMC)** Establish and maintain situational awareness of subordinate activity ISSM/ISSOs staffing issues and turnover; any potential negative impacts on SAP security management resulting from staffing and turnover will be routed to the Command ISSM. Maintain distribution lists to ensure effective dissemination of SAP policy, guidance, tasks, and awareness messages to enhance relations and communication across AFMC.

2.32.8. **(Added-AFMC)** Maintain a consolidated list of all Government SAP IT systems within Center SAP activities. Maintain the list in a central location as directed by the Command ISSM.

2.32.9. **(Added-AFMC)** Coordinate with the Center SSCI inspectors to validate/update the CSPO consolidated SAP IT system listing during SSCIs of subordinate SAP activities.

2.32.9.1. **(Added-AFMC)** The consolidated SAP IT system listing shall include, at a minimum, the following items:

2.32.9.2. **(Added-AFMC)** AFMC SAPF and SCIF ID as applicable.

2.32.9.3. **(Added-AFMC)** Organization/Office Symbol.

2.32.9.4. **(Added-AFMC)** DoD and DAF Unique Identifier.

2.32.9.5. **(Added-AFMC)** Information System Name.

2.32.9.6. **(Added-AFMC)** Identify if the system is a FENCES workload.

2.32.9.7. **(Added-AFMC)** Responsible ISSM or ISSO Name.

2.32.9.8. **(Added-AFMC)** Date and status (i.e., continuous or not) of last ATO.

2.32.9.9. **(Added-AFMC)** List of appointed ISSO(s) and Privileged Users to include name/grade, duty title, organization/office symbol, position (i.e., Contractor, ISSM/ISSO, etc.), and certifications.

2.33. **(Added-AFMC) SAP Security Compliance Inspectors shall:**

2.33.1. **(Added-AFMC)** Be appointed in writing by the Command GSSO.

2.33.2. **(Added-AFMC)** Complete the Command SSCI Training provided by the Command SSCIL, or designee prior to conducting inspections. Completion of the Center for Development of Security Excellence (CDSE) Orientation to SAP Security Compliance Inspections in residence course is recommended but not required. Completing the CDSE course does not replace the requirement to attend Command SSCI Training.

2.33.3. **(Added-AFMC)** Conduct SSCIs on behalf of and under the direction of the Command GSSO and AFMC/IG.

2.33.4. **(Added-AFMC)** Ensure all Command SAP activities are provided and utilize the most current SSCI checklist(s) to include any Special Emphasis Item (SEI) Checklists.

2.33.5. **(Added-AFMC)** Execute SSCIs consistent with applicable DoD and DAF SAP policies, this GM, and any applicable AFMC or IG processes and procedures.

2.33.6. **(Added-AFMC)** Execute and maintain a schedule of SSCIs. Incorporate travel budget projections by fiscal year when using AFMC SAPMO funds. Provide an updated SSCI schedule to AFMC/IG through the Command SSCIL no less than once per quarter.

2.33.7. **(Added-AFMC)** Coordinate with the Command SSCIL and applicable SSCI inspectors to conduct joint-inspections when more than one CSPO has inspection equity at an installation/location.

2.33.8. **(Added-AFMC)** Ensure SAP activities are aware of projected compliance inspections as early as possible. SAVs shall not be authorized within 180 days of a projected SSCI.

2.33.9. **(Added-AFMC)** Send formal inspection notification letter to inspected activity no later than 30 days prior to SSCI.

2.33.9.1. **(Added-AFMC)** Command SSCI notifications will be signed by the AFMC SAPMO Director or AFMC/IG and sent to the Center.

2.33.9.2. **(Added-AFMC)** Center SSCI notifications will be sent to the applicable PEO, Senior Material Leader (SML), and the Program Security Officer (PSO). If a SAP activity is not aligned under a PEO or SML, the SSCI notification will be sent to the applicable SAP accessed senior leader.

2.33.10. **(Added-AFMC)** As directed by the Command SSCIL, establish and maintain an AFMC SSCI Report Numbering system identifying all inspections subject to AFMC SAPMO oversight and assign a unique SAP inspection identification number.

2.33.11.**(Added-AFMC)** Document all deficiencies as part of the final SSCI Report, appropriately classifying deficiencies as either a finding or deviation, an observation, or a government actions item.

2.33.12. **(Added-AFMC)** Ensure final SSCI reports and associated CAPs are loaded into the Command SSCIL designated records repository. Locally maintain SSCI reports for a minimum of five (5) years to enable trends and analysis metrics.

2.33.13. **(Added-AFMC)** When a SSCI is expected to or does result in an overall marginal or unsatisfactory rating:

2.33.13.1.**(Added-AFMC)** The Command SSCIL will conduct all re-inspections of SSCI's resulting in an overall marginal or unsatisfactory rating.

2.33.13.2. **(Added-AFMC)** Notify the Command GSSO as soon as possible, but no later than 48 hours from inspection completion.

2.33.13.3. **(Added-AFMC)** Coordinate with the Command SSCIL to ensure notification and/or out-brief is provide to the Command GSSO, AFMC/IG, and the AFMC SAPMO Director.

2.33.13.4. **(Added-AFMC)** Ensure ACSP(s) and SAP activity Senior Leadership are notified of SSCIs resulting in an Unsatisfactory or Marginal rating, in any CFA, as an overall inspection result, and/or when deficiencies relate to OT&E shortfalls.

2.33.13.5. **(Added-AFMC)** Provide a copy of Unsatisfactory or Marginal final inspection reports to all stakeholders in coordination with the Command SSCIL, GSSO, and PSO.

2.33.13.6. **(Added-AFMC)** In coordination with the Command SSCIL, ensure the activity's PSO is notified of all Unsatisfactory or Marginal final inspection reports.

2.33.14. **(Added-AFMC)** Ensure SAP activities submit CAPs, as applicable, ensuring all deficiencies identified as findings are tracked through closure, enabling robust oversight and Command-level review of deficiency management of SAP activities.

2.33.15. **(Added-AFMC)** Collect, review, and track all CAPs. Ensure CAPs are updated and reviewed every 30 days from the previous report until all deficiencies have been corrected or a Plan of Action and Milestone has been submitted for items that cannot be corrected in a reasonable amount of time.

2.33.16. **(Added-AFMC)** Adhere to the processes identified is this GM as well as any other processes and guidance developed and disseminated by the Command SSCIL as defined in para 2.28.