DEPARTMENT OF THE AIR FORCE
WASHINGTON, DC

OFFICE OF THE SECRETARY

DoDM5205.07V1_DAFMAN16-703V1_DAFGM2024-01

29 APRIL 2024

MEMORANDUM FOR ALMAJCOM-FOA-DRU
DISTRIBUTION C

FROM: SAF/AA
1720 Air Force Pentagon
Washington, DC 20330

SUBJECT: Department of the Air Force Guidance Memorandum to DoDM5205.07V1_DAFMAN16-703V1, *DoD Special Access Program (SAP) Security Manual: General Procedures*

By Order of the Secretary of the Air Force, the 11 January 2023 Department of the Air Force Guidance Memorandum is extended. Compliance with this memorandum is mandatory. To the extent its directions are inconsistent with other Air Force publications; the information herein prevails, in accordance with DAFI 90-160, *Publications and Forms Management*.

This publication is applicable to the entire Department of the Air Force (DAF), including all uniformed members of the Regular Air Force, the United States Space Force, the Air Force Reserve, the Air National Guard, the Civil Air Patrol, when conducting missions as the official Air Force Auxiliary, all DAF civilian employees, and those with a contractual obligation to abide by the terms of DAF issuances.

Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AFI 33-322, *Records Management and Information Governance Program*, and 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 publishing of DoDM5205.07V1_DAFMAN16-703V1 permanently establishing this guidance, whichever is earlier.

EDWIN E. OSHIBA
Administrative Assistant

Attachment:
DoDM5205.07Vl DAFMAN16-703Vl_Enclosure 9: SAP Compliance Inspections

ENCLOSURE 9

SAP COMPLIANCE INSPECTIONS

1. GENERAL. The SAP security compliance process represents a unified and streamlined approach to the SAP security compliance inspections. All SAPs will be subject to the security compliance inspection process. The detailed guidance, procedures, Security Inspection Checklist for conducting security compliance inspections are posted on the website http://www.dss.mil/isp/specialprograms.html.

(Added) (DAF) Subsequent to the most recent change to DoDM 5205.07 Volume 1, the Defense Security Service (DSS) transitioned to the Defense Counterintelligence and Security Agency (DCSA). Some legacy links or references to DSS websites or pages may redirect but most are no longer valid. The current website for the Security Inspection Checklist is: https://www.dcsa.mil/Industrial-Security/Special-Access-Programs-Templates/

(Added) (DAF) The authorities to waive requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See DAFMAN 90-161, *Publishing Processes and Procedures*, for a description of the authorities associated with the Tier numbers. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the requestor's commander for non-tiered compliance items.

(Added) (DAF) Detailed guidance, procedures and checklists (e.g., Air Force (SAP) Security Compliance Self-Review Checklist, DoD SAP Checklist for Risk Management Framework Information Systems and the Department of the Air Force SAP Special Emphasis Items Checklist) are posted on the SAF/AAZ SharePoint for AF Security Personnel to access, https://usaf.dps.mil/teams/Security/SitePages/SharePoint%20for%20Security%20Personnel.aspx. Once completed they should be marked and protected according to the data enclosed.

(Added) (DAF) To ensure leadership (e.g., Directors, Commanders or Program Managers) awareness of their program security posture, Self-Reviews will be forwarded through leadership to the PSO, no later than 30 days after the review along with the 60-day corrective action plan if deficiencies are noted. Such action shall enable leaders to properly address any fiscal or other shortfalls related to the proper protection of their respective program(s). **(T-1)**

2. INSPECTION TYPES. Inspections are conducted to validate that SAP security processes and procedures are in compliance with the governing DoD policies and to ensure that the risk of compromise to SAP information is at a minimum. Inspections should be executed with the least amount of impact to the SAP, while maintaining a proficient, equitable, and comprehensive review.

a. There are four possible types of external inspections that can be conducted.

a. **(Added) (DAF)** Department of the Air Force adds two additional inspection types to the category.

(1) Core compliance inspections will be conducted at the direction of the inspection official, at a minimum every 2 years. The core compliance inspection consists of:

(a) Self-inspection checklist

(a) **(Added) (DAF)** Department of the Air Force (SAP) Security Compliance Self-Review Checklist and associated checklists. **(T-1)**

(b) Core functional areas (CFAs)

(b) **(Added) (DAF)** Core Compliace Items (CCIs) **(T-1)**

1. TS SAP data and materials accountability

2. SETA

3. Personnel security

4. Security management and oversight

5. Cybersecurity

6. Physical security

(c) Special emphasis items (SEIs)

(c) **(Added) (DAF)** Department of the Air Force SAP Special Emphasis Items Checklist. **(T-1)**

(2) Full scope inspections require a 100 percent validation of all functional areas. A full scope inspection will be conducted at the direction of the CA SAPCO when a less than satisfactory overall rating has been received as a result of a core compliance inspection. The most serious security rating, an unsatisfactory rating, is assigned when circumstances and conditions indicate that the program management personnel within the SAPF have lost, or are in danger of losing, their ability to adequately safeguard the classified material in their possession or to which they have access.

(3) Re-inspections are required when a less than satisfactory rating in one or more functional areas has been received. This can include just one or all functional area(s), SAP(s), or SEI(s). The re-inspection will be conducted no later than 90 days from the issuance of the final report.

(4) Unannounced or No Notice inspections can be full-scope or core compliance inspections conducted without notice and at the discretion of the CA SAPCO or designee.

(5) **(Added) (DAF)** Functional area inspections are conducted primarily on, but not limited to the areas that have received a less than satisfactory rating.

(6) **(Added) (DAF)** Higher Headquarters (HAF/MAJCOM/FLDCOM/FOA/DRU) Special Access Program Inspections. These inspections measure and report on the health, security, and compliance of SAP programs to the Secretary of the Air Force.

b. A security representative from the prime contractor should be present and participate during inspections of subcontractors. Designated personnel will serve as inspection team chiefs, assign ratings, conduct in or out briefings, or be responsible for completing the security inspection report.

c. Inspections will be coordinated among the SAPCOs and DSS when not carved out and conducted jointly to the greatest extent possible. Compliance inspections involving multiple SAP organizations will be fully coordinated between participating DoD organizations by the assigned team chiefs. Each organization is responsible for publishing its report.

3. SELF-INSPECTION. Self-inspections are required to be conducted annually by the GSSO, CPSO or designee, for all SAPFs for which they are assigned responsibility. Utilize the security compliance inspection template and document any deficiencies in a corrective action plan that addresses the plan for correcting deficiencies and areas deemed unsatisfactory as noted in the report. All supporting information will be included in the self-inspection report.

a. The documented results of self-inspections will be retained until the next government inspection is completed. All outstanding items must be completed before the destruction of any compliance documentation.

b. The documented results of the self-inspections will be submitted to the PSO for coordination within 30 days of completion. The PSO will be notified immediately if the self-inspection discloses the loss, compromise, or suspected compromise of SAP information.

c. In addition to the CFAs, inspectors will be required to validate SEIs. The CA SAPCO will annually determine the SEIs and report to the DoD SAPCO. The CA SAPCO will provide input on the trends and recommendations of the prior year to the DoD SAPCO.

4. STAFF ASSISTANCE VISIT (SAV). During a SAV, the PSO or designee will review security documentation and provide assistance and direction as necessary.

a. SAVs should be conducted as required and may include:

(1) Self-inspection checklists and corrective action plans.

(2) Outstanding government action items.

(3) Administrative security documentation (i.e., SOP, CPSO and IA manager appointment letter, OPSEC plan).

(4) Violations and infractions.

(5) SAP specific CI trends and briefings.

(6) SETA program.

(7) Physical security standards.

(8) Cybersecurity.

(9) TS accountability.

b. The PSO will provide a SAV report to the GSSO or CPSO detailing what was covered and identifying all actions requiring resolution. During this visit, the PSO will provide guidance and direction to the organization, which will assist in the development of an effective and standardized security program. The PSO will annotate and address any concerns that require follow up before the next inspection.

5. DEFICIENCIES. Once the inspection has been completed, the team chief will determine the rating of the inspection based on the number of deficiencies identified and the risk of a compromise to classified information. Deficiencies will be defined as a finding or deviation.

6. RATINGS. Inspections ratings are superior, commendable, satisfactory, marginal, and unsatisfactory.

a. If the rating is superior, commendable, or satisfactory, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days and place the organization on an inspection cycle not to exceed 24 month.

b. If the rating is marginal, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 30 days and schedule a re-inspection on the marginal areas within 90 days.

c. If the rating is unsatisfactory, the inspection official will discuss any deficiencies that may have been identified and provide the final inspection results in the SAP review report within 10 days and schedule a compliance security review to be conducted within 90 days.