



OFFICE OF THE SECRETARY OF DEFENSE

3200 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3000

January 7, 2016

MEMORANDUM FOR SPECIAL ACCESS PROGRAM (SAP) SENIOR WORKING GROUP

References: (a) DoDD 5205.07, "Special Access Program (SAP) Policy," July 1, 2010  
(b) DoDM 5205.07-V3, "DoD Special Access Program (SAP) Security Manual: Physical Security," April, 23 2015; Change 1, September, 21, 2015  
(c) CJCSI 3120.08D, "Integrated Joint Special Technical Operations (IJSTO)," January 28, 2013

This memorandum establishes the DoD SAPCO policy for DoD Oversight and Cognizant Authorities to implement for the reciprocity of DoD Special Access Program (SAP) facility accreditations. DoD Oversight and Cognizant Authorities and their designees are authorized to utilize any U.S. accredited SAP Facilities (SAPF), SAP Compartmented Areas (SAPCA) and Special Technical Operations Cells/Facilities (STOC/F) as SAP Working Areas (SAPWA) for all DoD SAPs.

- This includes handling, discussion and processing of non-persistent information. Non-persistent refers to any information the facility is not authorized to store, both digital and non-digital. This includes ensuring that information systems resident to the facility do not retain data locally beyond what the facility is approved for storing.
- Operating procedures must be implemented to ensure compartmentalization between guest activities and traditional daily operations. The sponsor initiating the guest activities within the facility is liable for ensuring that all individuals involved in the guest activity are appropriately cleared and accessed to the information planned to be discussed and/or processed.

It is the DoD Oversight and Cognizant Authorities and their designees responsibility to ensure the protection of DoD SAP information in all circumstances. This policy and implementation will facilitate the efficient use of DoD SAPFs and streamline redundant security practices. Ensure procedures are in place and ready to execute not later than 15 June 2016.

My point of contact for this matter is Mr. Paul Akerley, 703-695-7415, [paul.akerley.civ@mail.mil](mailto:paul.akerley.civ@mail.mil).

A handwritten signature in black ink, appearing to read "David B. Been", is located below the contact information.

David B. Been  
Brigadier General, USAF  
Director, DoD Special Access Program  
Central Office



OFFICE OF THE SECRETARY OF DEFENSE  
3200 DEFENSE PENTAGON  
WASHINGTON, DC 20301-3000

ACTION MEMO

December 10, 2015

FOR: UNDER SECRETARY OF DEFENSE (INTELLIGENCE)

FROM: Director, DoD Special Access Program Central Office *[Signature]*

SUBJECT: Approval for Use of DoD Special Access Program Facilities (SAPF) and Special Access Program Compartmented Areas (SAPCA) as Special Access Program Working Areas (SAPWA) for All DoD Special Access Programs (SAP)

References: (a) DoDD 5205.07, "Special Access Program (SAP) Policy," July 1, 2010  
(b) DoDM 5205.07-V3, "DoD Special Access Program (SAP) Security Manual: Physical Security," April 23, 2015

- Reference (a) directs me to coordinate with the USD (I) to ensure SAP security policy is appropriately reflected in DoD Issuances.
- Special access program facilities (SAPF) and special access program compartmented areas (SAPCA) are frequently accredited to support a specified SAP or a defined group of SAPs.
- Reference (b), issued under your cognizance, defines the processes and rigorous criteria for the accreditation of SAPFs or SAPCAs and specifies the criteria and parameters for establishment of a SAP Working Area (SAPWA).
  - IAW reference (b), Enclosure 3, Paragraph 1.e, once the SAPWA is "operational, only appropriately accessed SAP indoctrinated individual(s) will occupy them."
  - In keeping with reference (b), Enclosure 2, Paragraph 4, DoD Component Heads and OSD PSAs with Cognizant and Oversight Authority over SAPs, maintain the authority to implement this procedure.
- Approving any accredited SAPF, SAPCA, or Integrated Joint Sensitive Technical Operations (IJSTO) facilities defined for program use to act as a SAPWA for all DoD SAPs, facilitates the efficient use of DoD SAPFs and streamlines redundant administrative security practices.

RECOMMENDATION: Approve SAPFs, SAPCAs, and IJSTO facilities as SAPWAs for all DoD SAPs

Approve: *[Signature]* Disapprove: \_\_\_\_\_  
12/23/15

COORDINATION: Tab A

Prepared By: Jeffrey P. Spinnanger, OUSD (AT&L), Directorate of Special Programs, 703-697-4960