SAP SECURITY COMPLIANCE INSPECTION CHECKLIST

(VERSION: JANUARY 2026 v2)

1. ORGANIZATION NAME:		**Completion Date:**
2. ORGANIZATION LOCATION:		
3. ORGANIZATION PERSONNEL:	**GAM/CAM:**	
	GSSO/CSSO:	
	ISSO/ISSM:	
	PSM/PSO:	

This Department of War (DoW) SAP Security Compliance Inspection Checklist is to be used in accordance with DoD Manual 5205.07 when conducting SAP security compliance inspections or annual self-assessments. It applies to the Office of the Secretary of War (OSW), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the DoW, the Defense Agencies, the DoW Field Activities, and all other organizational entities within the DoW. It also applies to all OSW and DoW Component contractors and consultants who require access to DoW SAPs pursuant to the terms and conditions of the contract or agreement.

A. SECURITY MANAGEMENT

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
A-1	Has the CA SAPCO or designee formally appointed the GAM in writing to carry out the assigned duties? NOTE: Appointment letter must be provided during SAV/Inspection. (Government facilities only)	DoDM 5205.07, 3.1.d., Pg. 14	☐	☐	☐	
A-2	Has the CA SAPCO, CA SAPCO Security Director, Commanding Officer, GAM or designee formally appointed the GSSO in writing to carry out the assigned duties? NOTE: Appointment letter must be provided during SAV/Inspection. (Government facilities only)	DoDM 5205.07, 3.1.b.7. Pg. 13; 3.1.e.(2). (i)1. Pg. 17, Glossary Pg. 107	☐	☐	☐	
A-3	Has the GSSO been given any delegated authorities by the PSM or PSO? NOTE: If authorities delegated, review the delegation memorandum. (Government facilities only)	DoDM 5205.07, 3.1. f. (2). (a)-(d). Pg. 18	☐	☐	☐	
A-4	Has the CAM or appropriate industry official formally appointed the CSSO in writing to carry out the assigned duties? NOTE: Appointment letter must be provided during SAV/Inspection. (Industry facilities only)	DoDM 5205.07, 3.1. e. (2). (i)1. Pg. 17, 3.1.h.(2). Pg. 19, Glossary Pg. 105	☐	☐	☐	
A-5	If applicable to the inspected activity has the CA SAPCO formally appointed the AAA in writing to carry out the assigned duties?	DoDM 5205.07, 3.1. a. (12). Pg. 12, Glossary Pg. 104	☐	☐	☐	
A-6	Has the AAA performed Initial/Annual training on their authorities, standards, and limitations in accordance with CA SAPCO guidance? NOTE: Government facilities only.	DoDM 5205.07, 3.1. c. (3). Pg. 14	☐	☐	☐	

Controlled by:
Controlled by:
CUI Category:
Dissemination Control or Distribution Statement:
POC:

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
A-7	Has the ISSM been appointed in writing by their respective chain of command/leadership (e.g., Commander, Commanding Officer, PM, CIO, PSO, CAM or corporate equivalent)? NOTE: Appointment letter must be provided during SAV/Inspection.	JSIG 1.5.14, Pg. 1-20	☐	☐	☐	
A-8	Has the ISSO been appointed in writing by the authority at a site responsible for information system security (e.g., ISSM, Commander, Commanding Officer, PM, CIO, PSO, CAM or corporate equivalent)? NOTE: Appointment letter must be provided during SAV/Inspection.	JSIG 1.5.15, Pg. 1-21	☐	☐	☐	
A-9	Has the CA SAPCO, CA SAPCO Security Director, PSM, PSO, or if delegated, the GSSO, appointed the SPO in writing?	DoDM 5205.07, 3.1. b. (7). Pg. 13; 3.1.e.(2).(n). Pg. 17 3.1.f.(2). (a). Pg. 18	☐	☐	☐	
A-10	If required, has the GAM or CAM formally appointed the SAP Accountability Officer in writing? NOTE: Appointment letter must be provided during SAV/Inspection.	DoDM 5205.07, 3.1. i. Pg. 19	☐	☐	☐	
A-11	Has the GSSO or CSSO prepared a comprehensive SOP to implement security policies and requirements unique to the SAPF? Does the SOP contain at a minimum, all of the items listed in the DoDM? Has it been endorsed by the PSM or PSO and if applicable, approved by GAM or CAM? If the facility is a co-used SCIF, has the SOP been approved by the SCI Accrediting Official?	DoDM 5205.07, 3.2. a Pg. 20, 3.2.e.(1)-(10), 4.3.f.(3). Pg. 33, 4.8.b. Pg. 40, 15.9.c.(1). Pg. 95, ICD/ICS 705 Tech Specs (v1.5.1) 12.D.2. Pg. 93.	☐	☐	☐	
A-12	Has the GSSO or CSSO prepared a comprehensive EAP to implement security policies and requirements unique to the SAPF? Has it been endorsed by the PSM or PSO, and if applicable, approved by GAM or CAM? If the facility is a co-used SCIF, the EAP must be approved by the SCI Accrediting Official.	ICD/ICS 705 Tech Specs (v1.5.1) 12. M.	☐	☐	☐	
A-13	Is the EAP reviewed at least annually? Are all SAPF occupants familiar with the EAP? Are the EAP drills conducted and documented as circumstances warrant, but at least annually?	ICD/ICS 705 Tech Specs (v1.5.1) 12. M.6	☐	☐	☐	
A-14	Are all individuals assigned to or who have unescorted access to the SAPF familiar with and adhere to the SOP?	ICD/ICS 705 Tech Specs (v1.5.1) 12. D.3	☐	☐	☐	
A-15	Does the SAPF have an OPSEC Plan, is it reviewed annually, and updated at each lifecycle milestone or when missions dictate? Does it include the required topics?	DoDM 5205.07, 3.4.a.b. Pg. 21, DoDD 5205.02E	☐	☐	☐	
A-16	Have PPPs unique to the Program been developed and contain all required information? Has the PPP been submitted to the CA SAPCO?	DoDM 5205.07, 3.5.a.8 Pg. 22, 3.5.b. Pg. 22	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
A-17	Has the CAM submitted a program protection implementation plan to the PSM or PSO for all SAP activities associated with a contract? Does the implementation plan match any overarching OPSEC strategy or PPP? Was the program protection implementation guide signed by the GAM and PSM or PSO and submitted to the CA SAPCO?	DoDM 5205.07, 3.5.a.8 Pg 22, 3.5.c. Pg. 22	☐	☐	☐	
A-18	Has the GAM and PSM or PSO reviewed and endorsed annually, at minimum all PPPs under their cognizance to ensure compliance with DoDI 5000.83 requirements?	DoDM 5205.07, 3.5. a. (1)-(9) and 5.5.b, Pg. 22	☐	☐	☐	Review the PPP for required information and to validate annual review(s) (Government locations only)
A-19	Has the GAM maintained records of all technology transfers?	DoDM 5205.07, 3.1. d. (11). Pg 15; 11.1.b(1) Pg. 65	☐	☐	☐	If transfers have occurred, those records should be checked during the SAV/Inspection. (Government locations only)
A-20	Is SAP fraud, waste, abuse, and corruption (FWAC) information prominently displayed?	DoDM 5205.07, 3.1. e. (2). (m). Pg 17, 3.3.c, Pg. 21	☐	☐	☐	
A-21	Has the GSSO or CSSO conducted the annual self-inspection to include the Special Emphasis Items (SEIs)? Have the documented results been provided to the PSM/PSO within 30 days of completion? Did the report include a 60-day corrective action plan, and are updates provided every 30 days thereafter until complete?	DoDM 5205.07, 3.1. f. (2), Pg. 18, 8.4.b-c, Pg. 55	☐	☐	☐	
A-22	Is the PSM or PSO notified immediately if the self-inspection discloses the loss, compromise or suspected compromise of SAP information?	DoDM 5205.07, 8.4. c. Pg. 55	☐	☐	☐	
A-23	Are all documented results of self-inspections retained until the next external inspection is completed?	DoDM 5205.07, 8.4. a Pg. 55	☐	☐	☐	Results of previous self-inspections should be reviewed during the SAV/Inspection.
A-24	Has the PSM or PSO conducted a SAV at their discretion, as directed by the CA SAPCO, or if requested by the organization? Was the organizational leadership, GSSO or CSSO, SAP IS AOs), CA SAPCO, and any other applicable party as required provided a copy of the SAV report?	DoDM 5205.07, 8.5. Pg. 55	☐	☐	☐	
A-25	Have individuals accessed to SAP information notified the PSM/PSO/GAM/CAM/GSSO/CSSO if there have been any litigation actions that may pertain to a SAP, employee or union strikes, employer discrimination complaints, equal employment opportunity cases, Merit Systems Protection Board reconsiderations or other events that could affect the mission readiness, safety and security facility or cause a public disturbance?	DoDM 5205.07, 3.10. b. Pg. 25	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
A-26	Are all actual or potential security incidents reported in accordance with procedures, through organizational leadership to the PSM or PSO immediately, to the extent possible, and no later than 24 hours after discovery?	DoDM 5205.07, 7.1. a. (2). Pg..45	☐	☐	☐	
A-27	For security incidents, infractions, and inquiries that have occurred during this rating period: (1) Were SAP security professionals trained to handle/conduct security investigations? (2) Are incidents deemed as security infractions maintained locally by the GSSO/CSSO for review during compliance inspections? (3) Are all security incidents categorized as violations coordinated through the organizational leadership to the PSM/PSO for closure and additional action(s)? NOTE: Records of inquiries and their resolution should be checked during SAV/Inspections. (4) Has the PSM/PSO notified the GAM of any security incident involving CPI related to an SAP contract? (5) Does the security inquiry report address all required items? (6) Are initial security inquiry reports and initial recommendations for corrective action submitted to the CA SAPCO no later than 10 business days after receiving notification of a security incident?	DoDM 5205.07, 7.1.a.(1), (3), (4), Pg. 45, 7.1.a.(2), (b), Pg. 45, 7.2.a, Pg. 47, 7.2.b.(2) Pg. 48	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐	
A-28	Are inadvertent disclosure statements completed if personnel are determined to have had unauthorized or inadvertent access to SAP information?	DoDM 5205.07, 7.1.c Pg. 46	☐	☐	☐	
A-29	For all visits, is JADE or its successor used for access verifications if available? If unavailable, are written or electronic visits sent with all required information? If JADE or successor cannot be used for access verification has a written or electronic visit notification been sent before the visit containing: (1) Person's Name (2) Clearance level (3) Programs to be discussed (4) POC (5) Date of visit (6) Purpose	DoDM 5205.07, 9.1. Pg. 58, 9.7.a.(1-7). Pg. 60	☐	☐	☐	
A-30	Are non-SAP accessed visitors under constant escort by resident SAP accessed personnel in a SAPF?	DoDM 5205.07, 9.5. a. Pg. 59	☐	☐	☐	
A-31	Are non-SAP-cleared foreign nationals visiting a SAPF approved in advance by the CA SAPCO or designee?	DoDM 5205.07, 9.5. b. Pg. 59	☐	☐	☐	
A-32	Does the security officer or their designated representative immediately notify all recipients of the cancellation or termination of the visit request authorization for all debriefed personnel?	DoDM 5205.07, 9.6. Pg. 59	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
A-33	Has the GAM or designated representative approved all visits to SAPFs, or SAP activities associated with the Government contract? NOTE: If there is a designated representative inspectors should see the delegation artifact.	DoDM 5205.07, 9.1. a. Pg. 58 & 9.1.b. Pg. 58	☐	☐	☐	
A-34	Has the CAM or designee approved all visit between the prime contractor and their subcontractor(s)? NOTE: If there is a designee inspectors should see the delegation artifact.	DoDM 5205.07, 9.1. a. (1). Pg. 58				
A-35	Are visit requests in excess of 12 months not authorized unless approved by the PSO?	DoDM 5205.07, 9.1. Pg. 58	☐	☐	☐	
A-36	Have there been any Congressional visits? If yes, were they coordinated through the CA SAPCO and DoW SAPCO?	DoDM 5205.07, 9.8.a & b. Pg. 60	☐	☐	☐	
A-37	Is SAP material only reproduced on equipment approved by the PSM/PSO?	DoDM 5205.07, 4.8. a. Pg. 39	☐	☐	☐	
A-38	Have clear markings been placed on equipment to indicate if it can or cannot be used for reproduction of SAP material?	DoDM 5205.07, 4.8. a.(2). Pg. 39	☐	☐	☐	

A. SECURITY MANAGEMENT

COMMENTS:

B. PERSONNEL VETTING						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
B-1	Are all applicable personnel vetting files for each SAP-accessed individual maintained in JADE, or any successor system and include but are not limited to: (1) PSQs, PSQ Templates (as required) and supplemental information as required by the CA SAPCO. (2) DD Form 254 or consultant agreements for contractors, as necessary. (3) PARs. (4) Continuation of access (COA) approvals. (5) SAPIAs. (6) SETA records. (7) Foreign travel records. (8) Foreign contacts records, including personal, business, and suspicious contacts. (9) Inadvertent disclosure records. (10) Reports of security infractions and violations. (11) Potentially disqualifying information records. (12) LOCNs, as necessary.	DoDM 5205.07, 12.6. b & d.(1)-(12). Pg. 70, 14.5.a. Pg. 85	☐	☐	☐	
B-2	Do all nomination packages for access contain a completed PAR and PSQ completed within the last 365 days, supplemental information supporting "Yes" answers on the PSQ, and for contractors, a current PSO-validated DD Form 254?	DoDM 5205.07, 13.3. d. Pg. 78, Glossary	☐	☐	☐	
B-3	When an individual cannot meet minimum requirements for access, is a Letter of Compelling Need (LOCN) included in the package that describes the individual's unique skill/knowledge to support a determination that it is in the nation's best interest for the CA SAPCO to approve access?	DoDM 5205.07, 13.2. b. Pg. 77	☐	☐	☐	
B-4	Are Program Access Requests (PAR) approved by the AAA prior to the candidates signing the Special Access Program Indoctrination Agreement (SAPIA) and before formal indoctrination?	DoDM 5205.07, 12.3. c. Pg. 68	☐	☐	☐	
B-5	Have personnel temporarily assigned away from their home location for over 180 days been debriefed unless continued need-to-know has been approved in writing by the CA SAPCO?	DoDM 5205.07, 12.10. Pg. 72	☐	☐	☐	
B-6	Is the PSM/PSO notified when personnel no longer wish to work on SAPs, any person who refuses to sign the SAPIA, as well as changes of employment status for SAP-accessed personnel?	DoDM 5205.07, 12.9. Pg. 71	☐	☐	☐	
B-7	Has a SAPIA been executed at the time of the debriefing and uploaded to JADE or successor system or forwarded to PSM/PSO within three business days?	DoDM 5205.07, 12.12. c. Pg. 72, 12.12.c.(1), Pg. 73	☐	☐	☐	
B-8	Were any administrative debriefings performed during this inspection cycle, and if so, why? Were all attempts made to find the individual prior to executing an administrative debrief and was it reported as required?	DoDM 5205.07, 12.13 Pg. 74	☐	☐	☐	
B-9	Does the SPO forward the PSQ to the GAM if it contains derogatory information, reflected by a "Yes" answer, for a NTK determination, and make a recommendation to the PSM/PSO?	DoDM 5205.07, 13.4. c.(4). Pg. 80	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
B-10	On annual reviews of the PSQ's does the GSSO, CSSO, or SPO report derogatory information that was disclosed in a PSQ, but not previously reported, to the candidate's organizational security manager?	DoDM 5205.07, 13.5. e. (1). Pg. 81	☐	☐	☐	
B-11	Has the CSSO/GSSO informed the PSM/PSO of all reported adverse information that may affect the person's ability to protect program information?	DoDM 5205.07, 12.8., 12.9, Pg. 71	☐	☐	☐	
B-12	Is the GSSOs or CSSO performing the following for Official Travel: (1) Obtaining the notification of foreign travel and other relevant documentation by the SAP-accessed traveler before leaving? (2) Ensure personnel receive pre-travel threat awareness briefings and post-travel debriefings, using CI-support element provided products? (3) Informing the PSM or PSO about any travel related security issues identified by any SAP-accessed individual? (4) Filing all completed documentation in the SAP-accessed traveler's personnel vetting file? (5) Contacting their designated PSM or PSO when personnel report unofficial foreign travel to countries identified on the DoD SAPCO Consolidated Country Threat List or a travel advisory has been identified on the Department of State's Travel.State.Gov website and flagging these occurrences on the foreign travel reporting matrix. (6) Is written justification provided by the SAP accessed personnel to the GSSO or CSSO if the 14-business days requirement is not practical, for coordination with the PSM or the PSO and organizational leadership approval for foreign travel?	DoDM 5205.07, 14.2.a.(1). Pg. 82 14.2.b.(1)-(5). Pg. 82 & 83	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐	
B-13	Is the GSSO or CSSO performing the following for Unofficial Travel: (1) Verifying justification for travel requests reported with less than 30-day notice? (2) Reviewing all proposed foreign travel itineraries and in coordination with the PSM or PSO, request pre-travel, country specific threat awareness briefings and post-travel debriefings from CI personnel from the supporting Military Department counterintelligence organization (MDCO)? (3) Informing the PSM or PSO about any foreign travel, contacts, or security issues identified by any SAP-accessed individual?	DoDM 5205.07, 14.3.a.(1). Pg. 83 14.3.a.2,14.3. a. (4). Pg. 84 14.3.b.(1)-(5). Pg. 84 14.3.a.(2) Pg. 84	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
	(4) Filing all foreign travel requests in the SAP-accessed traveler's personnel vetting file? (5) Reporting any foreign travel trends to the PSM or PSO? Keeping the travel information will be maintained in a readily accessible form (i.e., a spreadsheet or database)?	DoDM 5205.07, 14.3.a.(1). Pg. 83 14.3.a.2,14.3. a. (4). Pg. 84 14.3.b.(1)-(5). Pg. 84 14.3.a.(2). Pg. 84	☐	☐	☐	

B. PERSONNEL VETTING

COMMENTS:

C. SECURITY EDUCATION						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
C-1	Has a SETA Program been established that meets the requirements and applies to all SAP-accessed individuals? Was it approved by the PSM/PSO?	DoDM 5205.07, 6.1. a-g, 6.2, Pg. 43	☐	☐	☐	
C-2	Has initial and annual training for all SAP accessed personnel been conducted and documented using CA SAPCO approved SAP training template? Was the training recorded using the SAP Training Record Template developed and provided by the CA SAPCO? Does it address all the topics identified? Was the record uploaded into JADE or its successor upon completion?	DoDM 5205.07, 6.4. a. b, e, Pg. 44	☐ ☐	☐ ☐	☐ ☐	
C-3	Has the initial/annual training been updated due to any changes? For example, changes in the SAP SCG relevant to the program, etc.	DoDM 5205.07, 6.4. a (1)-(4), Pg. 44	☐	☐	☐	
C-4	Have all SAP briefed personnel completed initial training and then annual training every 365 days thereafter?	DoDM 5205.07, 6.4. b, Pg. 44	☐	☐	☐	
C-5	Has HVSACO been included in initial training or indoctrination and annual security awareness refresher sessions?	DoDM 5205.07, 4.1. b. Pg. 30	☐	☐	☐	
C-6	Are SAP-accessed individuals briefed by the appropriate SAP security personnel, PSMs, PSOs, GSSOs, and CSSOs on individual reporting requirements during initial briefings and during annual training?	DoDM 5205.07, 6.4. d Pg. 44	☐	☐	☐	
C-7	Has the CA SAPCO required any supplemental, situational, or event-driven training? If so, that specific training provided to the inspected activity and conducted?	DoDM 5205.07, 6.4. f. Pg. 44	☐	☐	☐	
C-8	Has a formal debriefing program been developed that contains all the required information?	DoDM 5205.07, 12.12. a.-e. Pg. 72	☐	☐	☐	

C. SECURITY EDUCATION

COMMENTS:

D. ACCOUNTABILITY						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
D-1	Has the CA SAPCO or designee approved the accountability system? Does the accountability system address all nine (9) required items? Does the system account for all accountable SCI and collateral material, media, hardware, and equipment?	DoDM 5205.07, 3.1. i. (1) Pg. 19 4.3. a. (1)-(9) & 4.3.b, Pg. 32	☐	☐	☐	
D-2	Has the CA SAPCO directed the SAP Accountability Officer to account for all SECRET//SAR material, media, hardware, and equipment?	DoDM 5205.07, 3.1. i. (2) Pg. 19	☐	☐	☐	
D-3	Does the Accountability system record all transactions? If the accountability system is automated, is there a backup?	DoDM 5205.07, 4.3. b. Pg 32 4.3. c. (1)-(14) Pg. 32 & 33	☐	☐	☐	
D-4	Has an annual 100 percent inventory of accountable SAP classified material been conducted by the individual responsible for the control system or alternate and a disinterested party? Has the annual inventory been conducted within 365 days of the previous inventory?	DoDM 5205.07, 4.4. a. Pg. 34	☐ ☐	☐ ☐	☐ ☐	
D-5	Are inventories conducted by visual inspection of all items of accountable material and verification of pertinent information, including originator, date, subject, file number, and page count for TS//SAR documents held within the SAPF?	DoDM 5205.07, 4.4. a. (3). Pg. 34	☐	☐	☐	
D-6	Is a disclosure record for all TS//SAR items, regardless of format, available?	DoDM 5205.07, 4.3. d. Pg. 33	☐	☐	☐	
D-7	Is the disclosure sheet kept with the destruction paperwork and destroyed in accordance with the applicable records disposition schedule after the item is destroyed?	DoDM 5205.07, 4.3. d. (2). Pg. 33	☐	☐	☐	
D-8	Has the PSM or PSO authorized open storage of HVSACO material? NOTE: Provide authorization memorandum/instruction during SAV/Inspection.	DoDM 5205.07, 4.1. c. Pg. 30	☐	☐	☐	
D-9	Does the SAPF SOP address the user inactivity timeline "not to exceed 3 months," whereby user accounts on TS networks that have not logged in are suspended?	DoDM 5205.07, 4.3. f. (3). Pg. 33	☐	☐	☐	
D-10	Is all media, regardless of classification, recorded in a log, tracked going in/out of the SAPF, and inventoried annually?	DoDM 5205.07, 4.3. f. (4). Pg. 33	☐	☐	☐	
D-11	Are SAP working papers marked appropriately?	DoDM 5200.01 V2, Encl 3, 13. Pg. 41	☐	☐	☐	
D-12	Has the DoW SAPCO approved a percentage of the total accountable holdings to be inventoried due to a high volume of SAP materials?	DoDM 5205.07, 4.4. a. (1). Pg. 34	☐	☐	☐	
D-13	Are discrepancies between accountability records and annual inventories reported immediately to the GSSO or the CSSO and then to the PSM or PSO?	DoDM 5205.07, 4.4. b. Pg. 34	☐	☐	☐	
D-14	Are proper markings applied using source documents, security classification guides, or other guidance issued by the original classification authority?	DoDM 5200.01 V2, Encl. 3.2.a. Pg. 17, JSIG Control AC-17	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
D-15	Is the destruction of accountable classified program material and the completion of destruction certificates done by two program briefed personnel with access to both the classification level and each SAP? Is all Non-accountable SAP material destroyed by a SAP-briefed employee with access to both the classification level and each SAP included in the material being destroyed?	DoDM 5205.07, 4.9. a, 4.9.b, & 4.9.d.(2) Pg. 40	☐ ☐	☐ ☐	☐ ☐	
D-16	Have destruction certificates been completed and maintained in accordance with the approved records schedule?	DoDM 5205.07, 4.9.d.(2).(c) Pg. 41	☐	☐	☐	
D-17	Has the PSM or PSO approved alternate processes or procedures for verifying accountable items when verification of pertinent information is not feasible due to operational requirements? Has the alternate method been documented and reported to the CA SAPCO or designee security director?	DoDM 5205.07, 4.4.a.(4). Pg. 34	☐ ☐	☐ ☐	☐ ☐	
D-18	Are all SAP materials destroyed by approved methods and processes?	DoDM 5205.07, 4.9. Pg. 40	☐	☐	☐	

D. ACCOUNTABILITY

COMMENTS:

E. CYBER SECURITY						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
JSIG Control: Access Control (AC)						
E-1	Does your organization operate, maintain and/or support any SAP information system located within the facility that was authorized by any DoW SAP Component (i.e. locally managed ATO)? *[If "no", then proceed with completing Section E. If "yes", then the GSSO/CSSO and ISSM/ISSO are responsible for completing the SAP RMF checklist]*	DoD SAP Checklist for RMF Information Systems	☐	☐	☐	If organization locally manages its own Information Systems, then the SAP RMF Checklist should be made available to the inspector. If the organization primarily deals with External Information Systems (EIS) and does not manage their own Information Systems, then Section E will address administrative controls for local personnel.
E-2	Are local managers assigned to ensure account status (e.g. created, removed) for each Information System? If yes: does the account manager authorize or approve system, group, or role memberships for each user based on their usage of the system? Is the Account manager notified when a user's need to know for access changes or has ended (either for termination or transfer)? If a user no longer needs access, are there procedures in place to revoke the account within 24 hours? Does the account manager review system accounts for accurate levels of access annually? NOTE: This is applicable to any guest system within the facility, to include unclassified, collateral, or SCI networks (e.g. NIPR, SIPR, JWICS), enterprise SAP IT system, or platform SAP IT system.	AC-2, AC-6	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	
E-3	Is there local documentation or training that requires users to logout when workday has ended or during periods of extended absence (more than 6 hours)?	AC-2(5)	☐	☐	☐	
E-4	Are local shared/group accounts used? Are shared/group accounts approved in writing by the AO?	AC-2(9), AC-2(10)	☐	☐	☐	
E-5	If group accounts are utilized, are *local* procedures in place for changing or disabling accounts upon transfer, termination, or need to know change?	AC-2 (10)	☐	☐	☐	
E-6	Are accounts automatically disabled after 90 days of inactivity? If automatic disables are not configured, are there manual procedures in place to disable dormant accounts after 90 days?	AC-2 (3)	☐ ☐	☐ ☐	☐ ☐	
E-7	Are privileged user accounts and roles tracked and disabled when no longer appropriate?	AC-2 (7)	☐	☐	☐	
E-8	Is separation of duties in place for Data Transfer Agents (DTA's) and Media Custodians (MC's)? Is separation of duties in place for System Administrators and Audit Administrators?	AC-5, AC-6	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
E-9	Are wireless capabilities permitted within the SAPF? If so, are controls in place to disable wireless connectivity when not in use? If not, are all wireless capabilities removed prior to entry into the SAPF?	AC-18, AC-19	☐	☐	☐	
E-10	Are mobile devices permitted within the SAPF? Are procedures in place to mitigate vulnerabilities associated with the permitted mobile devices in the SAPF?	AC-19 AC-20(2)	☐	☐	☐	
E-11	Does the organization implement procedures to ensure portable Information System storage devices are authorized and documented? Does the organization have PSO approval for introduction and removal for portable storage devices to be used on Information Systems? Are PSO approved portable storage devices recorded in the accountability system?	AC- 20 (2)	☐	☐	☐	
JSIG Control: Awareness and Training (AT)						
E-12	Does the facility have role-based information systems training program implemented that cover the following roles: ISSO / ISSM? General User? Privileged User? Administrators? Data Transfer Agent (DTA)? Media Custodian (MC)? Other Specialized roles (i.e. ISSE)?	AT-1, AT-3	☐	☐	☐	
E-13	Is the training material reviewed annually for accuracy?	AT-2, AT-3	☐	☐	☐	
E-14	Are personnel trained initially and annually based on their roles?	AT-4, AU-11	☐	☐	☐	
E-15	Is training documented to include username, name of training, date of training, and type of training?	AT-4	☐	☐	☐	
E-16	Are training documents retained for a minimum of 5 years?	AT-1, AT-3	☐	☐	☐	
E-17	Do all users of IS within the SAPF have a signed user agreement (general user and/or privileged user) on file? Have all users who have signed a previous version of the user agreement read and resigned when the rules of behavior are revised/updated or at least annually?	AT-1, AT-3	☐	☐	☐	
JSIG Control: Incident Response (IR)						
E-18	Does the organization have a documented IS incident response policy (IRP) approved by the SAP Authorizing Official (AO)? Is the IRP reviewed at least annually? Is the IRP disseminated to all personnel?	IR-1 IR-3, IR-4, IR-5, IR-8, IR-9, PM-12	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
E-19	Does the IRP for IS include the following: Incident response testing? Incident handling procedures (preparation, detection and analysis, containment, eradication, and recovery)? Incident reporting and monitoring procedures? Insider threat? Spillage response? Incorporation of Lessons learned?	IR-3, IR-4, IR-5, IR-8, IR-9, PM-12	☐	☐	☐	
JSIG Control: Media Protection (MP)						
E-20	Does the organization have a Media Protection Policy (MPP) that addresses all media within the facility? Is the MPP reviewed at least annually? Is the MPP disseminated to all personnel?	MP-1	☐	☐	☐	
E-21	Does the MPP include the following items: Define roles and responsibilities for ISSM, ISSO, Media Custodian, Data Transfer Agent (DTA), and Systems Administrator? Appropriate media marking and labeling procedures in use for all media within the SAPF? Implementation of Malicious Code countermeasures. Including malicious code scanning to detect and quarantine, or eradicate malicious code that may be present on any removable media? Media Movement / Transport, day-to-day management and control?	MP-3, MP-4, MP-5, MP-6, SC-28, SI-3,	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	
E-22	Does the MPP include Media sanitization requirements?	DoD standards and reciprocity for sanitization of SAP IT devices, 20 Apr 2020 & MP-6	☐	☐	☐	
E-23	Is data at rest (DAR) encrypted with FIPS validated cryptography and NSA compliant cryptography?	SC-13, SC-18, NIST SP 800-171, FIPS Publication 140	☐	☐	☐	
JSIG Control: Data Transfers (AC, AT, MP)						
E-24	Does the organization conduct data transfers within the SAPF? If yes, does the organization have AO approved Assured File Transfer (AFT) procedures for all the following: Lateral transfers? Low-to-High? High-to-Low?	AC-4	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	
E-25	Are DTA's designated in writing, trained, and authorized to conduct data transfers within the SAPF?	AC-4, AT-3	☐	☐	☐	
E-26	Do procedures exist for information systems enforcing local dual authorization (e.g., two-person control) policy for all transfers of data from a classified computer to removable media?	AC-3(2)	☐	☐	☐	

JSIG Control: Auditing (AU)						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
E-27	Are all information systems configured to audit the events specified in JSIG AU-2 and protect audit information and tools?	AU-2	☐	☐	☐	
E-28	If site personnel are responsible to perform an audit review of the system, does the organization review IS audit records at least weekly for indications of unusual activity?	AU-9, AU-6	☐	☐	☐	
JSIG Control: Maintenance (MA, CM, SA)						
E-29	If site personnel are responsible to perform system maintenance, are system maintenance records maintained to reflect date, time, name of individual performing maintenance, description of the type of maintenance performed, and a list of hardware/software removed, replaced, or repaired?	MA-2	☐	☐	☐	
E-30	Does the organization implement a documented Configuration Management Plan including tracking all system components and inventories to prevent unauthorized and undocumented changes (or access) to system hardware/software?	CM-3, CM-8, CM-9	☐	☐	☐	

E. CYBER SECURITY

COMMENTS:

F. PHYSICAL SECURITY						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
F-1	Was the SAPF accredited in writing by a SAPF-AO designated by the CA SAPCO or designee?	DoDM 5205.07, 15.1. c. Pg. 86 & 15.7.c Pg. 92	☐	☐	☐	
F-2	Are periodic re-inspections conducted by the SAPF-AO based on threat, physical modifications, sensitivity of SAPs, and past security performance, but will be conducted no less frequently than every 3 years? Are the reports retained within the SAPF?	DoDM 5205.07, 15.7. c. Pg. 92	☐	☐	☐	
F-3	Does the facility have any waivers approved by the CA SAPCO?	DoDM 5205.07, 15.3.d. Pg. 89 15.4.a.(1) Pg. 89, ICS 705-1, H, Pg. 6	☐	☐	☐	
F-4	Has the SAPF-AO approved documented mitigations commensurate with the standards in the NCSC SCIF Specifications?	DoDM 5205.07, 15.6.a.(4), Pg. 91, ICD/ ICS 705 Tech Specs 1.5.1, Ch 2.2.(b). Pg. 4	☐	☐	☐	
F-5	Are the following documents retained for the life of the SAP facility: (2) Any accreditation documents (e.g., physical, TEMPEST, and ISs) and copies of any waivers granted by the CA SAPCO. (3) SAPF accreditation approval documentation, including mitigations and waivers. (4) TSCM reports for the entire period of SAPF accreditation. (5) Operating procedures and any security documentation, including IS security authorization packages, CUAs, appointment letters, MOAs, and emergency action plans.	DoDM 5205.07, 15.7.h.(1)-(5), 15.7.e. Pg. 92	☐	☐	☐	
F-6	Are SAPF areas constructed with true floor to true ceiling construction and STC requirements in accordance with ICD 705?	DoDM 5200.01 V3, Appendix to Encl. 3.1.b.(1). Pg. 45, ICD 705 Tech Specs, Ch 3.C.2.h). Pg. 13	☐	☐	☐	
F-7	If electronic processing occurs in the SAPF, (a) Has a TEMPEST countermeasure review been completed? (B) Has the CTTA determined TEMPEST countermeasures are required? (c) Were the CTTA recommended countermeasures implemented?	DoDM 5205.07, 15.13. Pg. 100	☐	☐	☐	
F-8	Has the GSSO/CSSO notified the PSO of any activity that affects the facility security clearance (FCL) or SAP accreditation?	DoDM 5205.07, 15.1.d.(2). Pg. 86	☐	☐	☐	
F-9	Where practicable, does the GSSO or CSSO maintain an access roster for all personnel who have unescorted access to the SAPF?	DoDM 5205.07, 15.9. a. Pg. 95	☐	☐	☐	
F-10	Have any medical devices or other portable electronic devices (PEDs) been approved for introduction and use in the SAPF? If yes, were all	DoDM 5205.07, 15.12. a. Pg. 97; ICD 124, ICD/ICS 705 Tech Specs 1.5.1, Ch 10.	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
	required approvals obtained before introduction of the device?		☐	☐	☐	
F-11	Are speakerphones and audio-conferencing systems used on unclassified telephone systems in the SAPF disabled? Has the PSM/PSO made exceptions to this requirement?	ICD 705 Tech Specs, Ch. 11.B.5.f). Pg. 84	☐	☐	☐	
F-12	Are the requirements for collaboration peripherals being adhered to?	DoDM 5205.07, 15.12. e. Pg. 97 & 98	☐	☐	☐	
F-13	Has the PSM/PSO or the designee determined whether an internal warning system or other additional methods (in accordance with SAPF SOP) needed to warn accessed occupants of the presence of non-accessed personnel or personnel without all the required SAP accesses for that space?	DoDM 5205.07, 9.5. c. (1). (2). Pg. 59	☐	☐	☐	
F-14	Does the SAPF have approved procedures for inspecting personal belongings and vehicles at the entry and exit points, or at other designated areas? Has legal counsel reviewed all inspection procedures before implementation?	DoDM 5205.07, 15.11. b. Pg. 97	☐	☐	☐	
F-15	Are combinations changed immediately whenever: (1) A combination lock is first installed or used? (2) A combination has been subjected, or believed to have been subjected to compromise? (3) Whenever an individual knowing the combination no longer requires access to it unless other sufficient controls exist to prevent access to the lock? (4) At other times when considered necessary by the PSM/PSO/GSSO/CSSO?	DoDM 5205.07, 15.10.b.(1)-(4). Pg. 96	☐	☐	☐	
F-16	Have all combinations been reset to 50-25-50 when the lock is taken out of service? Have combination padlocks been reset to the standard combination 10-20-30 when taken out of service?	DoDM 5205.07, 15.10. c. Pg. 96, DoDM 5200.01 V3, Encl 3, 11.b.(4). Pg. 40 & 41	☐	☐	☐	
F-17	Are all unserviceable high-security padlocks, keys, and cylinders controlled until properly destroyed.	DoDM 5205.07, 15.10. c. Pg. 96	☐	☐	☐	
F-18	Are all combinations to the SAPF entrance doors recorded on the Standard Form 700, "Security Container Information?	DoDM 5205.07, 15.10. d. Pg. 96	☐	☐	☐	
F-19	Are the SAPF entrance door(s) combinations stored in a different accredited SAPF (or when not feasible) stored in a location approved by the PSM/PSO/GSSO?	DoDM 5205.07, 15.10. d. Pg. 96	☐	☐	☐	
F-20	Are record(s) of the names of persons having knowledge of the combination being maintained?	DoDM 5200.01 V3, Encl 3, 11.a.(5). Pg. 40	☐	☐	☐	
F-21	Are security container and door combinations safeguarded at the highest classification of material authorized to be stored within the container or room? Is Part 1 of SF 700 personally identifiable information (PII) protected in an opaque envelope?	DoDM 5200.01 V3, Encl 3, 10.a. Pg. 39, DoDM 5200.01 V3, Encl. 3.11.a. Pg. 40	☐	☐	☐	
F-22	Are storage containers being inspected and logged prior to removal, repair, etc., by cleared personnel?	DoDM 5200.01 V3, Encl 3, 13. Pg. 41	☐	☐	☐	
F-23	Are security containers locked when not under the direct supervision of an authorized person entrusted with the contents?	DoDM 5200.01 V3, Encl. 3.11.(4). Pg. 40	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
F-24	Has the GSSO/CSSO issued and controlled all SAPF keys? Have locks been changed when a key is lost or is believed to be compromised?	ICD 705 Tech Specs, Ch.12. C.1.d) Pg. 91	☐	☐	☐	
F-25	Are end-of-day security checks properly annotated and retained using the SF 701 and SF 702?	DoDM 5200.01 V3, Encl. 2. 9. Pg. 19	☐	☐	☐	
F-26	Is the SAPF protected by an Intrusion Detection System (IDS) and tested semi-annually to ensure continued performance?	ICD 705 Tech Specs Ch. 7.A1.a). Pg. 60, Ch.7. D.3.b). Pg. 68	☐	☐	☐	
F-27	Are IDS test records properly documented with: testing dates, name of individuals performing the test, specific equipment tested, malfunctions detected, and corrective action taken and retained for two (2) years?	ICD 705 Tech Specs, Ch. 12.L.6. Pg. 98	☐	☐	☐	
F-28	Is each failure to arm or disarm the IDS system reported to the responsible SAPF GSSO/CSSO with records maintained for two years?	ICD 705 Tech Specs, Ch.7. B.3.c). Pg. 65	☐	☐	☐	
F-29	Does the primary entrance door IDS sensor/keypad have an initial time delay of 30 seconds or less?	ICD 705 Tech Specs, Ch.7. A.3.a).(6). Pg. 62	☐	☐	☐	
F-30	Does the SAPF IDS have a (UL) 2050 Standard certificate with Extent 3 installation for IDS components and monitoring stations? Note: US Government IDS systems developed and used exclusively by the USG, do not require UL 2050 certificate but must comply with UL2050 Extent 3 installation guidelines.	ICD 705 Tech Specs, Ch.7. A.2.(a-c). Pg. 60	☐	☐	☐	
F-31	Has the PSM/PSO approved an IDS Emergency Failure plan? Note: Plan may be included as part of PSM/PSO approved SOPs.	ICD 705 Tech Specs, Ch.7. A.1.e). Pg. 60	☐	☐	☐	
F-32	Is IDS installation and testing within the U.S. performed by U.S. companies using U.S. citizens? Is installation and testing outside of the U.S. performed by personnel who are U.S. TOP SECRET cleared, or U.S. SECRET-cleared and escorted by SAPF personnel?	ICD 705 Tech Specs, Ch.7. D.1.a). b). Pg. 68	☐	☐	☐	
F-33	Is equipment containing access-control software programs located in the SAPF or a SECRET controlled area or a SCIF?	ICD 705 Tech Specs, Ch. 8.C.4. Pg. 72	☐	☐	☐	
F-34	Are all fiber or metallic cables/wires that penetrate the SAPF labeled and properly identified? a. The accountability shall identify the precise use of every cable through labeling. b. Log entries may also be used. c. Designated spare conductors shall be identified, labeled, and bundled together.	ICD 705, Tech Specs, Ch.11. I.2.(a-c). Pg. 87	☐	☐	☐	
F-35	Are all unused conductors (all wires or fiber) removed from the facility or grounded?	ICD 705 Tech Specs, Ch. 11.I.3. Pg. 87	☐	☐	☐	
F-36	Is additional conduit penetration for future utility expansion conduit filled with acoustic fill and capped (end of pipe cover)?	ICD 705 Tech Specs, Ch. 3.G.6. Pg. 17	☐	☐	☐	
F-37	Are inspection port(s) installed outside the perimeter of the SAPF secured with an PSM/PSO/SAPF AO-approved high-security lock? Is this noted in the FFC?	ICD 705 Tech Specs, Ch.3. G.7.c). (5). Pg. 18 & 19	☐	☐	☐	
F-38	Does the Primary SAPF entrance door meet the required criteria?	ICD 705 Tech Specs, Ch.3. E.2.(a-b) and E.5, Pg 15	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
F-39	Do the Emergency Egress-only doors meet the required criteria?	ICD 705 Tech Specs, Ch 3.E.5, Pg. 15 & Ch.3. E.4.(a-d), Pg. 16	☐	☐	☐	
F-40	Are pass keys/by-pass keys strictly controlled by SAP indoctrinated personnel?	ICD 705 Tech Specs, Ch. 8.F.3. Pg. 73	☐	☐	☐	
F-41	Does the Alarm response time criteria for U.S. SAPFs meet: a. Response times for Intrusion Detection Systems (IDS) IAW 32 CFR Parts 2001 and 2004. a. Closed Storage response time of 15 minutes? b. Open Storage response time within 15 minutes of the alarm annunciation if the area is covered by SID or a five-minute alarm response time if it is not?	ICD 705, Tech Specs, Ch. 3.h(a-b), Pg. 19, 32 CFR Parts 2001 and 2004.	☐	☐	☐	
F-42	Are agreements established for external alarm monitoring, response, or both that include: (a) Response time for response forces and personnel? (b) Responsibilities of the response force upon arrival? (c) Maintenance of SAPF points of contact? (d) Length of time response personnel are required to remain on-site?	ICD 705 Tech Specs, Ch. 12.L.2. Pg. 98	☐	☐	☐	
F-43	Is the alarm monitoring station continuously supervised and operated by US citizens who are trained alarm monitors, eligible to hold a U.S. SECRET clearance?	ICD 705 Tech Specs, Ch. 7.B.6.b). Pg. 67	☐	☐	☐	
F-44	In the event of primary power failure, is there twenty-four hours of uninterruptible backup power provided by batteries, an uninterruptible power supply (UPS), generators, or any combination, that is also documented in the FFC?	ICD705 Tech Specs, Ch. 7.B.5.b) Pg. 66	☐	☐	☐	
F-45	Are there any Protected Distribution Systems (PDS) installed and/or connected to the facility? If yes, has the PDS been approved by the AO and documented? Is the PDS checked/monitored by cleared personnel in accordance with the documented approval or SOP?	CNSSI 7003 Section XI, Pg. 10-12	☐	☐	☐	
F-46	Has the PDS owner developed a SOP approved by the AO and the CSA which was submitted as part of the PDS approval documentation?	CNSSI 7003 Section XI, Pg. 10-12	☐	☐	☐	
F-47	Are PDS inspections conducted and documented as required?	CNSSI 7003 Section XI, Pg. 10-12	☐	☐	☐	
F-48	Is appropriate red/black separation in place as required?	PE-19, CNSSAM TEMPEST/1-13, D DM 5205.07, 15.13. .(3) Pg. 100	☐	☐	☐	
F-49	Have SAPTSWAs been approved and if so, are they being revalidated annually?	DoDM 5205.07, 15.3 Pg. 88	☐	☐	☐	

F. PHYSICAL SECURITY

COMMENTS:

G. CONTRACTING						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
G-1	Has a DD Form 254, Contract Security Classification Specification Requirements been prepared for each contractor performing work on DoW SAPs?	DoDM 5205.07, 10.1. Pg. 61	☐	☐	☐	
G-2	Are all documents associated with the contract (e.g., statement of work, performance work statement, or statement of objectives) safeguarded in accordance with the applicable SCG?	DoDM 5205.07, 10.1. Pg. 61	☐	☐	☐	
G-3	Does the DD Form 254 Contain: (1) An addendum that contains security guidelines and any HVSACO, collateral, or SAP-level information. (2) Any collateral and SCI requirements, including disposition of information, material, and facilities. (3) A listing of all security policy and procedural references applicable to the execution of the contract. (4) Explicit security guidance for contract execution. (5) The period of performance and specific authorized PIDs?	DoDM 5205.07, 10.1. a. (1)-(4). Pg. 61, 10.1.c.(1) Pg. 61	☐	☐	☐	
G-4	Are all prime contractors and subcontractors who require access to SAPs cleared pursuant to Part 117 of Title 32, CFR	DoDM 5205.07, 10.2. Pg. 62	☐	☐	☐	
G-5	Has the prime contractor obtained approval from the PSM/PSO, and the entity listed in Block 12 of the DD Form 254 before any release of SAP information?	DoDM 5205.07, 10.3. a. (1) Pg. 62	☐	☐	☐	
G-6	Prior to the release of SAP information has the prime contractor briefed any prospective subcontractor(s) regarding the procurement's enhanced special security requirements? Have arrangements for subcontractor program access been pre-coordinated with the PSM/PSO? Has the DD Form 254 been provided to the PSO for all subcontractors?	DoDM 5205.07, 10.3. b. (1-3) Pg. 62	☐	☐	☐	
G-7	Are contractors accessed to any individual PID/portfolio that are not identified on the SAP addendum?	DoDM 5205.07, 10.1. c. (2) Pg. 62	☐	☐	☐	
G-8	Are subcontractor DD Forms 254 signed by the subcontractor? Was the signature by an individual with the authority to obligate the subcontractor?	DoDM 5205.07, 10.1. d. Pg. 62	☐	☐	☐	
G-9	Has the Government Contracting Activity (GCA) and the GAM approved the use of SAP information for a contractor IR&D?	DoDM 5205.07, 10.4. a. Pg. 63	☐	☐	☐	
G-10	Upon contract close-out, are requests for retention of classified information submitted to the GCA & GAM through the PSM/PSO for review and approval? Has the contractor been authorized in writing by the GCA to retain any SAP information?	DoDM 5205.07, 10.5. b. (3) & (4). Pg. 63	☐	☐	☐	

ID#	Question	Reference, Policy	Yes	No	N/A	Remarks
G-11	Has the CSSO developed a termination plan for PSM/PSO approval at the initiation of a closeout, termination, or completion of a contract?	DoDM 5205.07, 10.5. c. Pg. 64	☐	☐	☐	
G-12	Have all relationships with subcontractors for SAP-related or security-related services been coordinated with the GCA and had a security review and endorsement by PSM/PSO?	DoDM 5205.07, 10.3. a. (3), Pg. 62	☐	☐	☐	

G. CONTRACTING

COMMENTS:

H. TRANSMISSION						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**
H-1	Has the GSSO or CSSO ensured compliance with the **order of precedence** for the transmission of SAP information and material?	DoDM 5205.07, 4.5. a(1)(a) -(e), Pg. 34	☐	☐	☐	
H-2	Has the PSM/PSO approved in writing the use of overnight delivery using USPS?	DoDM 5205.07, 4.5.a.(4)(a), Pg. 35	☐	☐	☐	
H-3	Is USG contract carrier (i.e. USPS Express Mail) used Monday through Thursday for transporting SAP information?	DoDM 5205.07, 4.5. a. (2). Pg. 35	☐	☐	☐	
H-4	Is all classified SAP material prepared and handled in accordance with DoDM 5200.01 V3?	DoDM 5205.07, 4.5. b. Pg. 36	☐	☐	☐	
H-5	Does the GSSO/CSSO or authorized designee provide detailed courier instructions, training, and courier authorization cards or letters annually to SAP briefed couriers for hand carrying SAP information?	DoDM 5205.07, 4.5. c. Pg. 36	☐	☐	☐	
H-6	Has the CA SAPCO or designee defined local travel and if so, are personnel complying with the requirement?	DoDM 5205.07, 4.5. c. (3). (a). Pg. 36	☐	☐	☐	
H-7	Do the locked courier pouch(es) have a tag or label with the courier's full name, organization, and telephone number?	DoDM 5205.07, 4.5. c. (3). (c). Pg. 36	☐	☐	☐	
H-8	Has the PSM/PSO approved the use of public transportation or ride share services?	DoDM 5205.07, 4.5. c. (4). Pg. 36	☐	☐	☐	
H-9	Has the PSM/PSO approved any exceptions for the two-person integrity requirement for couriering TS/SAR?	DoDM 5205.07, 4.5. c. (5). Pg. 36	☐	☐	☐	
H-10	Did any overseas hand-carrying of material occur during the current inspection cycle? Was it authorized by the CA SAPCO or their designee?	DoDM 5205.07, 4.6.b(3), Pg. 38	☐	☐	☐	
H-11	Has the transport of SAP material unable to be hand carried been approved by the PSM/PSO and does the transportation plan include all required information?	DoDM 5205.07, 4.5.d.(1). Pg. 37, 4.5.d.(2)(a) -(e) Pg. 37	☐	☐	☐	
H-12	Does the courier authorization memorandum contain all of the required information?	DoDM 5205.07, 4.5. c. (9), Pg. 37	☐	☐	☐	
H-13	Is there documented PSM/PSO approval or PSM/PSO issued written procedures for all reproduction devices used in a SAPWA or SAPTSWA? Is reproduction equipment used in a SAPWA or SAPTSWA positioned so it can be continuously monitored?	DoDM 5205.07, 4.8. c. Pg. 40	☐	☐	☐	

H. TRANSMISSION
COMMENTS:

I. SPECIAL EMPHASIS ITEMS						
ID#	**Question**	**Reference, Policy**	**Yes**	**No**	**N/A**	**Remarks**

I. SPECIAL EMPHASIS ITEMS

COMMENTS: