SECURITY COMPLIANCE INSPECTION TEMPLATE

(Version: November 14, 2017)

Facility/Program Name: _____

Reviewer Name: _____ Date Completed: _____

This Department of Defense Security Compliance Inspection Checklist is to be used as described in DoD Manual 5205.07-V1 when conducting self-assessments and applies to all DoD Components including the OSD, 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 Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities and their authorized contractors within the DoD. Each checklist should be marked with the appropriate security classification markings and declassification instructions. **Core Functional Areas (CFAs) are identified in *blue italic font*.** (Note: In addition to the references provided in the tables below, local Activity or individual Agency/Component/Service policy, procedures, and/or regulations may also apply).

A. SECURITY MANAGEMENT

ID #	Questions	References	Yes	No	N/A	Remarks
A-1	Does the SAO recommend waivers of physical security safeguards to the Director, CA SAPCO or designee for approval based on a risk assessment and operational requirements?	DoDM 5205.07-V3, Encl. 1.d; Encl. 3.5.a.6, and Encl. 2.5.b	☐	☐	☐	
A-2	Did the Director, CA SAPCO approve waivers for imposing safeguards exceeding a standard, prior to implementation, even when the additional safeguards are based on risk?	DoDM 5205.07-V3, Encl. 3-1.d	☐	☐	☐	
A-3	Has the PSO approved and documented mitigations commensurate with the requirements of ICD-705 technical specifications?	DoDM 5205.07-V3, Encl. 3-5.a.5	☐	☐	☐	
A-4	Are trained and knowledgeable GSSOs or CPSOs, appointed in writing by GPM and CPMs respectively, to serve as the SAP security official at each organization or facility?	DoDM 5205.07-V1, Encl. 3-4; and V1 Glossary	☐	☐	☐	
A-5	Are copies of GSSO/CPSO appointment letters provided to the PSO and maintained on file within the SAPF?	DoDM 5205.07-V1, Encl. 3-2.i; V1-Glossary	☐	☐	☐	
A-6	Is the ISSM/ISSO appointed in writing by their respective chain of command/leadership?	JSIG 1.5.14, 1.5.15, and AT-3	☐	☐	☐	

Classified By:

Derived From: SCG

Reason: E.O 13526, Section 1.4

Declassify On: 31 Dec 20 (Per FSE 20150306)

ID #	Questions	References	Yes	No	N/A	Remarks
A-7	Have comprehensive SOPs been developed to implement the security policies & requirements unique to the SAPF?	DoDM 5205.07-V1, Encl. 4-1(a)	☐	☐	☐	
A-8	Are all individuals assigned to or with unescorted access to the SAPF familiar with and adhere to the SOP?	ICD 705 Tech Specs Ch. 12, d.3	☐	☐	☐	
A-9	Have maintenance procedures been written and incorporated into the SOP listing the actions necessary when non-SAP briefed maintenance technicians' work on the equipment?	DoDM 5205.07 –V1, Encl. 5.11.a	☐	☐	☐	
A-10	Are SOPs with changes, and proposed SOPs forwarded to the PSO for approval?	DoDM 5205.07-V1, Encl. 4.1.b	☐	☐	☐	
A-11	Has an annual self-inspection been conducted by CPSO/GSSO or designee and did it address issues reflected in the Security Compliance Inspection Template?	DoDM 5205.07-V1, 3.3.f, and Encl. 9.3(a-c)	☐	☐	☐	
A-12	Were Special Emphasis Items (SEIs) obtained through the CA SAPCO and documented during the self-inspection?	DoDM 5205.07-V1, Encl. 9.3.c	☐	☐	☐	
A-13	Are self-inspection reports submitted to the PSO within 30 days following completion of the inspection?	DoDM 5205.07-V1, Encl. 9.3.b	☐	☐	☐	
A-14	Is the PSO notified immediately if the inspection discloses the loss, compromise or suspected compromise of classified material?	DoDM 5205-07.V1, Encl. 9.3.b	☐	☐	☐	
A-15	Are documented results of self-inspections retained until the next government inspection and not destroyed until after all outstanding items are completed?	DoDM 5205.07-V1, Encl. 9.3.a	☐	☐	☐	
A-16	Is the current SAP FWAC telephone number prominently displayed throughout each SAPF?	DoDM 5205.07-V1, Encl. 4.3.b	☐	☐	☐	
A-17	Are instances of Government or Industry fraud, waste, abuse and corruption reported through "SAP" channels designated by the PSO, and are individuals notified that collateral FWAC channels must not be used for SAP information?	DoDM 5205.07-V1, Encl. 4.3	☐	☐	☐	
A-18	Are MOUs, MOAs, CUAs and ISAs signed and current?	DoDM 5205.07-V1, Encl. 4.4, 4.12.b; JSIG AC-20, CA-3, SA-9	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
A-19	a. Is the SAPF shared between the government and another organization? b. If multiple SAPs are located within a SAPF, has a Co-Utilization Agreement been executed between PSOs prior to occupancy? c. Have the responsible cognizant security officers approved the Co-Utilization Agreement? d. Has authorization from the cognizant PSO and the Special Security Officer (SSO) been obtained for co-utilization of SCI within a SAPF, or SAP within a SCIF?	DoDM 5205-07-V1, Encl. 3.1.d	☐	☐	☐	
A-20	Is the SAP prepared to comply with USG treaties and agreements without unnecessary SAP exposure during verification activities?	DoDM 5205.07-V1, Encl. 4.8.a, DoDD 2060.1	☐	☐	☐	
A-21	Has the organization implemented an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recover?	JSIG: IR-4.c	☐	☐	☐	
A-22	Are all security violations reported immediately, and no later than 24 hours of discovery to the PSO?	DoDM 5205.7-V1, Encl. 8.a	☐	☐	☐	
A-23	Has the PSO provided oversight for collateral classified material and has it been approved by the PSO before introduction, inclusion, or production into the SAPF?	DoDM 5205.07-V1 Encl. 5.6.a	☐	☐	☐	
A-24	Has the SAP security official of the affected SAPF determined the scope of the corrective action taken in response to a security infraction/violation and reported it to the PSO for approval?	DoDM 5205.07-V1, Encl. 8.b	☐	☐	☐	
A-25	Are security infractions documented and made available for review by the PSO during visits?	DoDM 5205.07-V1, Encl. 9-4.a.4; V1, Encl. 8; 5200.01 and V3, Encl. 6.3.f.2	☐	☐	☐	
A-26	Has the organization employed a formal sanctions process for personnel failing to comply with established information security policies and procedures?	DoDM 5205.07-V1, Encl. 8, DoDM 5200.01-V3, Encl.6-6.d.3	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
A-27	a. Has the PSO determined the SAP facility warrants an OPSEC survey? (If yes, answer A-27 (b) and (c)) b. Are threat-based comprehensive OPSEC surveys conducted by Subject Matter Experts every 3 years? c. Based upon OPSEC survey results, has the CPSO/GSSO developed and maintained an OPSEC program that identified vulnerabilities and developed countermeasures?	DoDD 5205.02E, Encl. 2.11.g; DoDD5205.02 Glossary	☐	☐	☐	

B. PERSONNEL SECURITY

ID #	Questions	References	Yes	No	N/A	Remarks
B-1	Does the GSSO/CPSO maintain personnel security files for each SAP-accessed individual with all required documentation?	DoDM 5205.07-V2, Encl. 3-7	☐	☐	☐	
B-2	Do PAR requestors possess a SAP access level at least equal to the nominated individual being submitted?	DoDM 5205.07 V2, Encl. 3-3(a) & (c)	☐	☐	☐	
B-3	Has the CPSO/GSSO reported all adverse information, changes in employee status, foreign travel, foreign contact etc., to the PSO that may affect the person's ability to protect program information?	DoDM 5205.07-V1, Encl. 4-2(a-e), DoDM 5205.07-V2, Encl. 3-9	☐	☐	☐	
B-4	Is all travel outside the continental U.S., Hawaii, Alaska, and U.S. territories (e.g., Puerto Rico) reported to the GSSO/CPSO in advance?" [30 days in advance for non-official travel and as soon as practical prior to official government travel]	DoDM 5205.07-V2, Encl. 5-2, and 5-3	☐	☐	☐	
B-5	Are Foreign Travel briefings and debriefings conducted and documented for all accessed personnel prior to and upon return from travel?	DoDM 5205.07-V2, Encl. 5-2 and Encl. 5-3	☐	☐	☐	
B-6	Are country-specific threat awareness briefings provided based on the DIA foreign intelligence threat level, or other CA SAPCO guidance?	DoDM 5205.07-V2, Encl. 5-2 and Encl. 5-3	☐	☐	☐	
B-7	Have personnel temporarily assigned away from their home location for over more than 60 days been debriefed unless continued need-to-know has been approved in writing by the CA SAPCO?	DoDM 5205.07 V2, Encl. 3-11	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
B-8	Does the GSSO/CPSO notify the PSO when personnel no longer wish to work on SAPs, report any person who refuses to sign the SAPIA, as well as changes of employment status for SAP-accessed personnel?	DoDM 5205.07-V2, Encl. 3-10	☐	☐	☐	
B-9	Have personnel determined to have had unauthorized or inadvertent access to classified SAP information: (1) Been interviewed to determine the extent of the exposure, and;	DoDM 5205.07-V1, Encl. 8.d	☐	☐	☐	
	(2) Been requested to complete an Inadvertent Disclosure Form based on the extent of the exposure?		☐	☐	☐	
B-10	Has the GSSO/CPSO notified the PSO of any activity that affects the facility security clearance (FCL) or SAP accreditation?	DoDM 5205.07-V3, Encl. 3.1.g	☐	☐	☐	
B-11	Do SAP-accessed personnel have a valid need-to-know and certification that he/she will materially and directly contribute to the Program?	DoDM 5205.07-V2, Encl. 3-3.a.2 and Encl. 4.1; DoDM 5205.11 5.b	☐	☐	☐	
B-12	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-V2, Encl. 3.4.a and Encl. 4.3.a.	☐	☐	☐	
B-13	Has a SAPIA been executed at the time of the debriefing and forwarded to PSO within three business days?	DoDM 5205.07-V2, Encl. 3.13.c	☐	☐	☐	
B-14	Has the GSSO/CPSO established, conducted, and documented an initial indoctrination briefing for all individuals accessed to a SAP?	DoDM 5205.07-V1, Encl. 3.3.e	☐	☐	☐	
B-15	Has a formal debriefing program been developed?	DoDM 5205.07-V2, Encl. 3.13	☐	☐	☐	
B-16	If attempts to locate an individual either by telephone or mail are not successful, and the whereabouts of the individual cannot be determined in 30 days; is the individual administratively debriefed (i.e., completion of a debriefing form, annotating the form with "INDIVIDUAL NOT AVAILABLE-ADMINISTRATIVELY DEBRIEFED")? Is the appropriate database updated to reflect this?	DoDM 5205.07-V2, Encl. 3.14	☐	☐	☐	
B-17	Does the individual's nomination package contain a completed PAR, an executed pre-screening questionnaire dated within one year (365 days) and supplemental information supporting "Yes" answers?	DoDM 5205.07-V2, Encl. 4.3.d	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
B-18	Has the responsible SPO reviewed the nomination package for completeness and accuracy and validated that the candidate meets the criteria for SAP access?	DoDM 5205.07-V2, Encl. 3-3(b) and Encl. 4.4.c	☐	☐	☐	
B-19	When an individual cannot meet DoDM 5205.07-V2 Encl. 4-2 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-V2, Encl. 3.1.g	☐	☐	☐	
B-20	Are candidate nomination packages that contain a "Yes" response to the pre-screening questionnaire forwarded to the PSO for action, and are non-concur actions documented on the PAR in the remarks section?	DoDM 5205.07-V2, Encl. 3.3.c.1	☐	☐	☐	
B-21	Are Program Access Rosters (or electronic database) maintained for all SAP Facilities?	DoDI 5205.11 Encl. 7-1.h	☐	☐	☐	
B-22	Has each SAP briefed individual annually revalidated access eligibility by either recertifying answers provided to the pre-screening questionnaire and any supplemental information provided; or by completing a new prescreening questionnaire with previously unreported potentially disqualifying information reported to their local security officer?	DoDM 5205.07-V2, Encl. 4.5.b	☐	☐	☐	

C. ACCOUNTABILITY

ID #	Questions	References	Yes	No	N/A	Remarks
C-1	Has a Top Secret Control Official (TSCO) been appointed in writing by the government or contractor PM when the PSO determines a program requires one?	DoDM 5205.07-V1, Encl. 3.5	☐	☐	☐	
C-2	Has all accountable SAP information been entered into a PSO approved document control accountability system to record all transactions of handling, receipt, generation, reproduction, destruction, and when dispatched either internally or externally to other SAPFs?	DoDM 5205.07-V1, Encl. 5.4.a.b	☐	☐	☐	
C-3	Are processes used by the TSCO thoroughly documented in the SOP?	DoDM 5205.07-V1, Encl. 3.5	☐	☐	☐	
C-4	Does the accountability system assign individual responsibility for all accountable information?	DoDM 5205.07-V1, Encl. 5.4.b	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
C-5	Is a disclosure sheet (access record) maintained for each TS SAP item and signed by each individual who viewed the document?	DoDM 5205.07-V1, Encl. 5.4.d	☐	☐	☐	
C-6	Has an annual 100 percent inventory of accountable SAP classified been conducted by the individual responsible for the control system or alternate and a disinterested party?	DoDM 5205.07-V1, Encl. 5.5	☐	☐	☐	
C-7	Are these inventories conducted by visually inspecting all items of accountable SAP material and verification of pertinent information, copy and page count for TS SAP held within the SAPF?	DoDM 5205.07-V1, Encl. 5.5.a	☐	☐	☐	
C-8	Are results of the annual accountable inventory and any discrepancies reported immediately to the PSO?	DoDM 5205.07-V1, Encl. 5.5.b	☐	☐	☐	
C-9	Is each item of TOP SECRET SAP material numbered in series and identified with an individual copy number and total copy count?	DoDM 5205.07-V4, Encl. 2.2.g	☐	☐	☐	
C-10	Are working papers dated when created, marked, controlled, and safeguarded with the highest classification of any information contained?	DoDM 5205.07-V4, Encl. 2.2.i	☐	☐	☐	
C-11	Are all working papers containing SAP information either entered into the accountability system or destroyed after 30 calendar days from the date of origin?	DoDM 5205.07-V4, Encl. 2-2.i; DoDM 5200.01-V2, Encl. 3.13.a	☐	☐	☐	
C-12	Has the PSO approved 100% control and accountability measures for all media (regardless of classification)?	DoDM 5205.07-V1, Encl. 5.3; USD(I)/DoD CIO: Insider Threat Memorandum, 12 July 2013	☐	☐	☐	
C-13	Is the two-person integrity rule for controlling all media being complied with when introduced to secure facilities?	USD(I)/DoD CIO: Insider Threat Memorandum, 12 July 2013	☐	☐	☐	

D. CLASSIFICATION AND MARKING

ID #	Questions	References	Yes	No	N/A	Remarks
D-1	Is a security classification guide maintained and accessible for each program within the SAPF?	DoDM 5205.07-V4, Encl. 2.1.a	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
D-2	Are challenges to SAP classified information and/or material classifications forwarded through the PSO to the appropriate Original Classification Authority (OCA)?	DoDM 5205.07-V4, Encl. 2.1.d	☐	☐	☐	
D-3	Is public release of SAP information not authorized without written permission from the government?	DoDM 5205-07-V1, Encl. 5.10(a) & (b)	☐	☐	☐	
D-4	Do you have SAP information that has been approved for public release?	DoDM 5205-07-V1, Encl. 5.10	☐	☐	☐	
D-5	Do individuals report any attempts by unauthorized personnel to obtain SAP information immediately to the PSO or GPM?	DoDM 5205-07-V1, Encl. 5.10.a	☐	☐	☐	
D-6	Has all SAP material been classified IAW the program SCG?	DoDM 5205.07-V4, Encl. 2.1 & 2.2	☐	☐	☐	
D-7	Is each section, part, paragraph or similar portion of a classified document marked to show the highest level of its classification or that the portion is unclassified?	DoDM 5205.07-V4, Encl. 2.2.e	☐	☐	☐	
D-8	Is Unclassified HVSACO information safeguarded IAW established procedures?	DoDM 5205.07-V1, Encl. 5.1	☐	☐	☐	

E. REPRODUCTION

ID #	Questions	References	Yes	No	N/A	Remarks
E-1	Is program material only reproduced on equipment approved by the PSO?	DoDM 5205.07-V1, Encl. 5.11.a	☐	☐	☐	
E-2	Have the CPSO/GSSOs prepared written reproduction procedures?	DoDM 5205.07-V1, Encl. 5.11.a	☐	☐	☐	
E-3	Is approved reproduction equipment positioned to be continually monitored when it is outside the SAPF?	DoDM 5205.07-V1, Encl. 5.11.b	☐	☐	☐	
E-4	Has a notice indicating if equipment can or cannot be used for reproduction of classified material been posted?	DoDM 5205.07-V1, Encl. 5.11.a	☐	☐	☐	
E-5	Are procedures approved in writing by the PSO (including clearing of equipment, accessing of operators, clearing of media, handling malfunctions, etc.) when reproduction equipment is used outside a SAPF (i.e. TSWA)?	DoDM 5205.07-V1, Encl. 5.11.b	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
E-6	When a controlled document is reproduced, is the new product marked (e.g. Copy A, Copy 2A, Copy 1, etc.) indicating the number of times it has been copied, or has the copy been given a separate accountability number?	DoDM 5205.07-V4, Encl. 2.2.g	☐	☐	☐	

F. DESTRUCTION

ID #	Questions	References	Yes	No	N/A	Remarks
F-1	Has the PSO reviewed and approved all destruction procedures including NSA/CSS approved destruction equipment?	DoDM 5205.07-V1, Encl. 5.12	☐	☐	☐	
F-2	Are two program briefed personnel destroying accountable classified program material and completing destruction certificates?	DoDM 5205.07 V1, Encl. 5.12	☐	☐	☐	
F-3	Are destruction records maintained for 5 years?	DoDM 5205.07-V1, Encl. 5.12.a & Encl. 5.4.d	☐	☐	☐	
F-4	Is all classified waste destroyed as soon as possible (not allowing materials to accumulate beyond 30 days unless approved by the PSO)?	DoDM 5205.07-V1, Encl. 5-12	☐	☐	☐	

G. *PHYSICAL SECURITY*

ID #	Questions	References	Yes	No	N/A	Remarks
G-1	Has the SAPF been formally accredited in writing by a designated SAP Accrediting Official (SAO) prior to conducting any SAP activities?	DoDM 5205.07-V3, Encl. 3.1.b	☐	☐	☐	
G-2	Are periodic re-inspections (no less than every 3 years) conducted based on threat, physical modifications, sensitivity of SAPs, and past security performance?	DoDM 5205.07-V3, Encl. 3.6	☐	☐	☐	
G-3	Has an accreditation checklist (e.g., SAPF Fixed Facility Checklist or Compartmented Area Checklist) been completed and approved by the SAO or designee?	DoDM 5205.07-V3, Encl. 3.4	☐	☐	☐	
G-4	Has the cognizant SAO approved preconstructions plans for any construction expansion or modifications to the SAPF?	DoDM 5205.07-V3, Encl. 3.4	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
G-5	Does the SOP contain guidance for control of PEDs and other items introduced to or removed from the SAPF, T-SAPF, SAPCA, SAPWA, and SAPTSWA?	DoDM 5205.07-V3, Encl. 3.11.a	☐	☐	☐	
G-6	Are Personal Electronic Devices (PED), with the exception of the following, prohibited within a SAPF: (1) Electronic calculators, spell checkers, language translators, etc.	DoDM 5205.07-V3, Encl. 3.11.b	☐	☐	☐	
	(2) Receive-only pagers.		☐	☐	☐	
	(3) Audio and video playback devices.		☐	☐	☐	
	(4) Receive only Radios.		☐	☐	☐	
	(5) Devices that do not transfer, receive, store, or generate data (text, audio, video, etc.).		☐	☐	☐	
G-7	Are entry/exit inspections procedures, reviewed by legal counsel, documented in procedures and conducted to deter the unauthorized removal of classified material and deter the introduction of prohibited items or contraband?	DoDM 5205.07-V3, Encl. 3.10	☐	☐	☐	
G-8	When conditions warrant, has a TSCM evaluation been requested (at the discretion of the SAO)?	DoDM 5205.07-V3, Encl. 3.6.b	☐	☐	☐	
G-9	Are combinations changed immediately whenever: (1) A combination lock is first installed or used?	DoDM 5205.07-V3, Encl. 3.9	☐	☐	☐	
	(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 PSO?		☐	☐	☐	
G-10	Where there is co-utilization of SCI within a SAPF, or SAP within a SCIF, has authorization from the PSO & the servicing SSO been obtained?	DoDM 5205.07-V1, Encl. 4.4.d	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
G-11	Are security containers locked when not under the direct supervision of an authorized person entrusted with the contents?	DoDM 5205.07-V1, Encl. 5-3(d); DoDM 5200.01-V3, Encl. 3.3; ICD 705, Tech Specs, Ch. 2.c.5.b	☐	☐	☐	
G-12	Are SF702, Container Check Sheets properly annotated?	DoDM 5205.07-V1, Encl. 5.3.d	☐	☐	☐	
G-13	Is the SAPF protected by an Intrusion Detection System (IDS) and tested semi-annually IAW ICD 705?	DoDM 5200.01-V3, Encl. 3(a-b); ICD 705 Tech Specs Chapter 7.d.3.b	☐	☐	☐	
G-14	Are IDS test records properly documented with: test date, name of person performing the test, specific equipment tested, malfunctions detected, and corrective action taken?	ICD 705, Tech Specs, Ch. 12.L.6	☐	☐	☐	
G-15	Are the alarm test records maintained for 2 years?	ICD 705, Tech Specs, Ch. 12.L.6	☐	☐	☐	
G-16	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.3.6	☐	☐	☐	
G-17	Does the SAPF IDS have a current (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)	☐	☐	☐	
G-18	Has the PSO approved an IDS Emergency Failure plan? Note: Plan may be included as part of PSO approved SOPs	ICD 705, Tech Specs, Ch. 7.a.1.e and Ch. 12.a.1.f.	☐	☐	☐	
G-19	Is the installation and testing of the IDS conducted by US citizens? (Note: Non-US citizens shall not provide these services without prior written approval by the PSO)	ICD 705, Tech Specs, Ch. 7.d.1	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
G-20	Is equipment containing access-control software programs located in a minimum Secret controlled area, and are the IDS and Access Control Systems (ACS) Administrators briefed to either SCI for SCIFs (SAPCA) or to a SAP for non-SCI stand-alone SAPFs?	ICD 705, Tech Specs, Ch. 7.a.3.c.2.h & Ch. 8.b.1	☐	☐	☐	
G-21	Are security container and door combinations safeguarded at the highest classification of material stored within the container or room?	DoDM 5205.07-V3, Encl. 3.9.e	☐	☐	☐	
G-22	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; ICD 705 Tech Specs Ch. 9.b.	☐	☐	☐	
G-23	Are all walls finished and painted from true-floor-to ceiling? (e.g. to provide visual evidence of unauthorized penetrations)	ICD 705, Tech Specs, Ch. 3.c.2.h, 3.C.3.e.5, 3.c.3.f.6	☐	☐	☐	
G-24	Are fiber or metallic cables/wires that penetrate the SAPF labeled and properly identified?	ICD 705, Tech Specs, Ch. 11.I.2.a	☐	☐	☐	
G-25	Are all unused conductors (all wires or fiber) removed from the facility or grounded?	ICD 705, Tech Specs, Ch. 11.I.3	☐	☐	☐	
G-26	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	☐	☐	☐	
G-27	Is the SAPF entry door equipped with a lock that meets FF-L-2740A requirements (CDX-07, 8, 9, 10 or S&G 2740)? If no, and the SAP area resides within a SCIF (e.g. SAPCA), is SAP access control accomplished through mechanical or electronic access control devices? *Note: Spin-dial combination locks are not installed on SAPCA doors*	DoDM 5205.07-V3, Encl. 3-8(c)&(d); IC.D 705, Tech Specs, Ch. 3.E1.a, Ch. 8.b.4	☐	☐	☐	
G-28	Are GSA safes labeled with "General Services Administration Approved Security Container," affixed to the front of the container?	DoDM 5200.01-V3, Encl. 3.8	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
G-29	Are end-of-day security checks conducted and documented?	DoDM 5200.01-V3, Encl. 2.9 and DoD 5220.22-M, 5.102	☐	☐	☐	
G-30	Are all unclassified speakerphones disabled?	ICD 705, Tech Specs, Ch. 11.b.5.f.	☐	☐	☐	
G-31	When a badge system is considered necessary, has it been documented in the facility SOP & addressed topics such as badge accountability, storage, inventory, disposition, destruction, format & use?	DoDM 5205.07-V3, Encl. 3.8.b.1	☐	☐	☐	
G-32	If electronic processing occurs in the SAPF; (a) Has a TEMPEST countermeasure review been completed? (b) If yes to B-2(a), has the CTTA determined TEMPEST countermeasures are required? (c) If yes to B-2(b), did the CTTA recommend the most cost-effective countermeasure that will contain compromising emanations within the inspectable space?	DoDM 5205.07-V3, Encl. 3.1.b.2.f, DoDM 5205.07-V3, Encl. 3.12.c	☐ ☐ ☐	☐ ☐ ☐	☐ ☐ ☐	
G-33	When the TEMPEST countermeasure review is complete, has the PSO issued specific guidance in accordance with national directives?	DoDM 5205.07-V3, Encl. 3.12.a	☐	☐	☐	
G-34	Is the Emergency Action Plan (EAP) reviewed annually?	ICD 705, Tech Specs, Ch. 12.m.5	☐	☐	☐	

H. ACCESS CONTROL

ID #	Questions	References	Yes	No	N/A	Remarks
H-1	Is a written/electronic visit notification approved prior to visiting a SAPF (via hardcopy/electronic transfer/database)?	DoDM 5205.07-V1, Encl. 10.1	☐	☐	☐	
H-2	Has the GPM or his/her designated representative approved all visits between program activities (excluding visits between sub and prime)? Has the PSO or designee verified the accesses to the facility?	DoDM 5205.07-V1, Encl. 10.1	☐	☐	☐	
H-3	Are visit requests in excess of twelve-months not authorized unless approved in writing by the PSO?	DoDM 5205.07-V1, Encl. 10.4	☐	☐	☐	
H-4	Are all visit requests transmitted via PSO-approved channels (via hardcopy/electronic transfer/database)?	DoDM 5205.07-V1, Encl. 10.1	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
H-5	Has the CPSO/GSSO or his/her designated representative immediately notified all recipients of the cancellation or termination of visit requests?	DoDM 5205.07-V1, Encl. 10.7	☐	☐	☐	
H-6	Is positive identification of each visitor made using an official State or Federal-issued identification card/credential with a photograph?	DoDM 5205.07-V1, Encl. 10.5	☐	☐	☐	
H-7	Are non-program accessed visitors continuously escorted and their movements closely controlled by SAP accessed personnel while in a SAPF?	DoDM 5205.07-V1, Encl. 10.6.a	☐	☐	☐	
H-8	Are Foreign Nationals visiting the SAPF approved by the CA SAPCO or designee?	DoD 5205.07-V1, Encl. 10-6.b	☐	☐	☐	
H-9	Are advance arrangements coordinated between the visitor, the visitor's cognizant security officer and the destination facility's security officer regarding the hand carrying of program material?	DoDM 5205.07-V1, Encl. 10.2	☐	☐	☐	
H-10	Has the PSO or designee determined whether an internal warning system is necessary to warn accessed occupants of the presence of non-briefed personnel (e.g. rotating light beacons) or employed along with other additional methods (e.g., verbal announcements) to warn or remind personnel of the presence of un-cleared personnel?	DoDM 5205.07-V1, Encl. 10.6.c	☐	☐	☐	
H-11	Are all non-program briefed personnel (e.g., maintenance workers, repair technicians, etc.) required to complete the visitor's record and be escorted by a resident program-briefed individual?	DoDM 5205.07-V1, Encl. 10.6.a & Encl. 10.8	☐	☐	☐	
H-12	Has a separate program visitor's record been established for program briefed visitors? Does it show the visitor's first and last name, authorized credential identification number, citizenship, organization or firm, date visited, purpose, time in and out, and sponsor on the log?	DoDM 5205.07-V1, Encl. 10.8	☐	☐	☐	
H-13	Are program discussions conducted only in approved SAPFs?	DoDM 5205.07-V3, Encl. 3.1 & 3.2	☐	☐	☐	

I. *COMPUTER SECURITY*

ID #	Questions	References	Yes	No	N/A	Remarks
I-1	Does any information system processing occur within the facility (i.e., are there any computers located within the facility) regardless of classification? **[*If "NO," then skip the rest of Section I.* *If "YES," then complete section I}***	JSIG, PE-16	☐	☐	☐	
I-2	Are each of the systems located in the SAPF authorized to operate (e.g., Do external information systems and/or guest systems and/or collateral systems have valid approvals to operate within the facility)?	JSIG, CA-2, SA-9	☐	☐	☐	
I-3	Is appropriate red/black separation in place as required?	DoDM 5205.07-V3, Encl. 3.12.d.3; JSIG PE-19; CNSSAM TEMPEST/1-13	☐	☐	☐	
I-4	Does a media protection policy exist that addresses: (1) ALL media in the facility (e.g., CD/DVDs, hard drives, tape drives, USB drives, etc.)?	DoDM 5205.7-V1, Encl. 6 & JSIG, MP-1	☐	☐	☐	
	(2) Media movement/transport, day-to-day management and control?		☐	☐	☐	
I-5	Does the organization implement and maintain malicious code countermeasures, including malicious code scanning to detect and quarantine, or eradicate malicious code that may be present on any removable media?	JSIG, MP-1, MP-6 & SI-3	☐	☐	☐	
I-6	Are appropriate media marking and labeling procedures in use?	JSIG, MP-3 DoDM 5205.07, V4, Encl. 6	☐	☐	☐	
I-7	Are system maintenance records maintained to reflect date, time, name of individual performing the maintenance, description of the type of maintenance perfomed, and a list of the hardware/software removed, replaced or repaired?	JSIG, MA-2	☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
I-8	Does a formal **initial and annual** IA Training Program exist that addresses duties/responsibilities of: (1) ISSMs/ISSOs (2) System, Network and/or Database Admins (3) Data Transfer Agents (DTA/DTO) (4) General Users (5)Other Specialized IA Training (e.g., ISSE)	Privileged: JSIG, AT-3 General: JSIG, AT-2 & AT-3 PL-4	☐	☐	☐	
			☐	☐	☐	
			☐	☐	☐	
			☐	☐	☐	
			☐	☐	☐	
I-9	Have both General Users and Privileged Users signed respective Access Agreement and Acknowledgement of Responsibilities forms, and are they reviewed/updated at least annually or upon departure of an employee	JSIG, AT-3, PL-4 & PS-6	☐	☐	☐	
I-10	Are duties of individuals with IS access separated to prevent malicious activity without collusion? (e.g. System Administrators shall not perform security audit functions, DTAs shall not perform media custodian duties without AO approval)	JSIG, AC-5	☐	☐	☐	
I-11	Are all Information Systems configured to audit the events specified in JSIG AU-2 and protect audit information and tools?	JSIG, AU-2 and AU-9	☐	☐	☐	
I-12	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?	JSIG, CM-3, CM-8 & CM-9	☐	☐	☐	
I-13	Does your organization operate, maintain and/or support any SAP information system located within the facility that was authorized by any DoD SAP Component? ***[If "no", then proceed directly to Section K.*** ***If "yes", then the GSSO/CPSO and ISSM/ISSO are responsible for completing the SAP RMF checklist]***	DoD SAP Checklist for RMF Information Systems	☐	☐	☐	

J. TRANSMISSION

ID #	Questions	References	Yes	No	N/A	Remarks
J-1	If transmission by a commercial courier is anticipated, has the PSO approved its use?	DoDM 5205.07-V1, Encl. 5.7.a.3	☐	☐	☐	
J-2	Is all classified SAP material prepared, reproduced, and packaged by program-briefed personnel in SAPFs?	DoDM 5205.07-V1, Encl. 5.7.b	☐	☐	☐	
J-3	Are receipts for the transmission of all classified (SECRET/TOP SECRET) material used and retained for 5 years?	DoDM 5205.07-V1, Encl. 5.4.c.11 & 5.7.b (1-2); Retention Guidelines	☐	☐	☐	
J-4	Has the recipient of classified material been contacted when acknowledgment of a shipment of material is not returned within 15 days?	DoDM 5205.07-V1, Encl. 5.7.b.4	☐	☐	☐	
J-5	Are GSSO/CPSO providing detailed courier instructions and training to SAP briefed couriers when hand carrying SAP information?	DoDM 5205.07-V1, Encl. 5.7.5.e	☐	☐	☐	
J-6	Are Courier Authorization letters or card *(see below)* issued by the CPSO/GSSO from the departure location outlining the courier procedures? (1) Does the Courier Authorization and pre-departure instructions address the: a) method of transportation, b) travel itinerary (intermittent/ unscheduled stops, remain-overnight scenarios, etc.), c) specific courier responsibilities (primary/alternate roles-as necessary), and d) completion of receipts (as necessary) and full identification of the classified data being transferred and e) a discussion of emergency/contingency plans (include after-hours POCs, primary/alternate contact data, telephone numbers, etc.)	DoDM 5205.07-V1, Encl. 5-7.e.4.a (1-5) & 5-7.e.4.b	☐	☐	☐	
	(2) Has each courier acknowledged receipt/understanding of this briefing in writing?		☐	☐	☐	
	(3) In the case of experienced program-briefed individuals who frequently or routinely perform duties as classified couriers, are they issued Courier Authorization cards by the CPSO in lieu of individual letters for each trip?		☐	☐	☐	
	(4) Are courier cards revalidated/reissued annually?		☐	☐	☐	

ID #	Questions	References	Yes	No	N/A	Remarks
J-7	Is Top Secret material transmitted only by authorized means (e.g., 2-person courier, PSO approved single courier, or secure electronic means)?	DoDM 5205.07-V1, Encl. 5.7.a(1-6); DoDM 5205.07-V1, Encl. 5.7.e.1	☐	☐	☐	
J-8	Is SAP information double-wrapped using opaque material which precludes observation of contents?	DoDM 5205.07-V1, Encl. 5.7.b.3(a-b)	☐	☐	☐	
J-9	Does the GSSO/CPSO oversee transmission of SAP material?	DoDM 5205.07-V1, Encl. 5.7.a	☐	☐	☐	
J-10	When secure facsimile is permitted, has the PSO approved it in writing? When electronic transmission is permitted, did the authorizing official, in coordination with the PSO approved the system in writing?	DoDM 5205.07-V1, Encl. 5.2(b-c)	☐	☐	☐	
J-11	When a U.S. Postal mailing channel is approved by the PSO, is mail received only by appropriately cleared and accessed personnel?	DoDM 5205.07-V1, Encl. 5.7(d)	☐	☐	☐	
J-12	Are problems, miss-deliveries, losses, or other security incidents encountered with courier of SAP information immediately reported to the PSO?	DoDM 5205.07-V1, Encl. 5.7(e)	☐	☐	☐	
J-13	Before any movement of classified SAP assets are transportation plans developed and approved by the PSO at least 30 days in advance of the proposed movement?	DoDM 5205.07-V1, Encl. 5.9	☐	☐	☐	

K. *SECURITY EDUCATION*

ID #	Questions	References	Yes	No	N/A	Remarks
K-1	Has the GSSO/CPSO established a SETA program for their SAP and has the PSO approved it?	DoDM 5205.07-V1 Encl. 7.3.a; DoDM 5205.07-V1 Encl. 7.2	☐	☐	☐	
K-2	Have GSSO/CPSOs ensured initial and annual refresher Security Education and Training program meets specific and unique requirements of individual SAPs as well as addressing all topics on the training record template?	DoDM 5205.07-V1, Encl. 7.3, 7.4.a & 7.4.b.1	☐	☐	☐	

L. CONTRACTING

ID #	Questions	References	Yes	No	N/A	Remarks
L-1	Has a DD Form 254, Contract Security Classification Specification Requirements been prepared for each contractor performing work on DoD SAPs?	DoDM 5205.07-V1, Encl. 11	☐	☐	☐	
L-2	When a subcontractor does not have the requisite facility clearance, has the prime CPSO or designee submitted an FCL request to DSS?	DoDM 5205.07-V1, Encl. 11.2	☐	☐	☐	
L-3	In the pre-contract phase, has the prime contractor advised the prospective subcontractor (prior to any release of SAP information) of the procurement's enhanced special security requirements? Have arrangements for subcontractor program access been pre-coordinated with the PSO?	DoDM 5205.07-V1, Encl. 11.3.b	☐	☐	☐	
L-4	Has the Subcontractor Supplier Data Sheet that includes the reason for considering a contractor, and DD Form 254 been provided to the PSO for all subcontractors?	DoDM 5205.07-V1, Encl. 11.3.b	☐	☐	☐	
L-5	Are DD Form 254s prepared by prime contractor CPSOs and forwarded to the PSO for approval (before signature by the prime contractor and release to subcontractors)?	DoDM 5205.07-V1, Encl. 11.1	☐	☐	☐	
L-6	Have the provisions of DoDM 5205.07, SAP Security Manual, Volumes 1-4 been added to the DD254, consultant agreements upon contract award or modification?	DoDM 5205.07-V1, Encl. 11.1.a	☐	☐	☐	
L-7	In lieu of DD Form 254's, are memorandum of agreement (MOA) or interagency agreements established between the DoD and Non-DoD U.S. Government (USG) departments, activities, agencies, and all other organizational entities that require access to DoD SAPs?	DoDM 5205.07-V1, 2.c	☐	☐	☐	
L-8	Upon contract close-out, are requests for retention of classified information submitted to the Government Contracting Officer (GCO) through the PSO for review and approval?	DoDM 5205.07-V1, Encl. 11.7.a	☐	☐	☐	

M. GUARD FORCE

ID #	Questions	References	Yes	No	N/A	Remarks
M-1	For CONUS CLOSED storage SAPF, is a response force capable of responding to an alarm within 15 minutes of annunciation? For CONUS SAPF OPEN storage, is a response force capable to respond to an alarm; (1) Within 15 minutes when Security In Depth (SID) is approved by the PSO or SAO? Or; (2) Within 5 minutes when there is insufficient Security In Depth as determined by the PSO or SAO?	ICD 705, Tech Specs, Ch. 3.h(a-b)	☐ ☐	☐ ☐	☐ ☐	
M-2	Are MOAs established for external alarm monitoring, response, or both that include; • Response time for response forces and personnel? • Responsibilities of the response force upon arrival? • Facility maintenance points of contact? • Length of time response personnel are required to remain on-site?	ICD 705, Tech Specs, Ch. 12.L.2	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	☐ ☐ ☐ ☐	
M-3	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	☐	☐	☐	
M-4	Is guard response testing accomplished and documented?	ICD-705, Tech Specs, Ch. 12.L.7	☐	☐	☐	

N. SPECIAL EMPHASIS ITEMS						
Code / No.	**Question**	**References**	**Yes**	**No**	**N/A**	**Remarks**
N-1			☐	☐	☐	
N-2			☐	☐	☐	
N-3			☐	☐	☐	
N-4			☐	☐	☐	
N-5			☐	☐	☐	