**(U) SPECIAL ACCESS PROGRAM (SAP) RISK MANNAGEMENT FRAMEWORK (RMF)**

**CYBERSECURITY COMPLIANCE CHECKLIST**

***Version 1.1***

**Reviewer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_**

**Organization: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ System: \_\_\_\_\_\_\_\_\_\_\_\_\_**

**(U) This checklist does not replace the AO/DAO-approved SSP or SCTM for a particular system. Evidence of system specific continuous monitoring results for a system can be provided to satisfy these self-assessment requirements if the scope of continuous monitoring assessments includes the items on this checklist.**

(U) This checklist serves as an aid for the inspection and assessment of information systems, networks, and components under the purview of the Department of Defense (DoD) Special Access Program Central Office (SAPCO) and DoD Service/Agency SAPCOs. Based on the criteria specified within the JSIG, this checklist may be used **in conjunction with the SAP Security Compliance Checklist** in preparation for formal inspections and staff assistance visits.

**Instructions: Check Yes or No based on your self-assessment of the organization and/or system(s) implementation**

**Enter “S” for SCTM into the Yes column if deviations from the JSIG requirements exist that are approved in the SCTM**

**Enter “P” for POA&M in the No column if deviations are documented in a POA&M that has been accepted by the AO**

| **ID#** | **Questions** | **References** | **Yes** | **No** | **N/A** | **Remarks** |
| --- | --- | --- | --- | --- | --- | --- |
| **ROLES AND RESPONSIBILITIES** | | | | | | |
| 1 | Are the ISSM, and/or ISSO appointed to their position and performing their responsibilities as per the JSIG? | JSIG 1.5.14;  JSIG 1.5.15 |  |  |  |  |
| 2 | Are privileged users adhering to, and performing their duties, as per their established role-based responsibilities, acceptable system use agreement, privileged user guides, etc.? | JSIG 1.5.16; JSIG PL-4; JSIG PS-6 |  |  |  |  |
|  | | | | | | |
| **POLICY AND PROCEDURES** | | | | | | |
| 3 | Have tailored controls been reviewed at least annually as part of the continuous monitoring program? | JSIG Chapter 3, Page 3-43 |  |  |  |  |
|  |  |  |  |  |  |  |
| **ACCESS CONTROL** | | | | | | |
| 4 | Are procedures in place for (a)creating, (b)activating, (c)modifying, (d)monitoring, (e)disabling, and (f)removing accounts that comply with provisions outlined in the JSIG? | JSIG AC-2 |  |  |  |  |
| 5 | Are accounts reviewed **at least annually** for changes in personnel status? | JSIG AC-2 |  |  |  |  |
| 6 | Are all accounts which have been inactive **for a minimum of 90 days** automatically disabled? | JSIG AC-2(3) |  |  |  |  |
| 7 | If the site has unattended processing requirements, are the procedures (1) Documented? | JSIG SSP 3.1 |  |  |  |  |
| (2) Approved by the AO/DAO? | JSIG AC-11 |  |  |  |  |
| (3) Implemented as approved? | JSIG AC-3 |  |  |  |  |
| 8 | If the site has periods processing requirements are the procedures (1) Documented? | JSIG SSP 4.0; JSIG SC-4; JSIG SC-4(2) |  |  |  |  |
| (2) Approved by the AO/DAO? | JSIG SSP 4.0; JSIG; SC-4; JSIG SC-4(2) |  |  |  |  |
| (3) Implemented as approved? | JSIG AC-3 |  |  |  |  |
| 9 | Are procedures for all manual Data Transfers between IS, also known as Assured File Transfers (AFT):  (1) Documented? | JSIG AC-4 |  |  |  |  |
| (2) Approved by the AO/DAO? | JSIG AC-4 |  |  |  |  |
| (3) Implemented as approved? | JSIG AC-3; JSIG AC-4 |  |  |  |  |
| 10 | Are duties of individuals with SAP IS access separated to prevent malicious activity without collusion? (At a minimum, system administrators shall not also perform security audit functions, and DTAs shall not perform media custodian duties without explicit AO/DAO approval.) | JSIG AC-5 |  |  |  |  |
| 11 | Is the principle of least privilege implemented and enforced, allowing only authorized accesses for users that are necessary to accomplish assigned tasks, and is assignment of privileged use reviewed on a **quarterly** basis? | JSIG AC-6; JSIG AC-6(7) |  |  |  |  |
| 12 | Are **privileged users (except the DTA role)** required to use separate, non-privileged accounts when performing non-privileged functions? | JSIG AC-6(2) |  |  |  |  |
| 13 | Are the number of super user (administrator/root) accounts strictly limited to the maximum extent possible? | JSIG AC-6(5) |  |  |  |  |
| 14 | Are user accounts locked after **a maximum of 3** unsuccessful logon attempts within a **15 minute time period** requiring an administrator to unlock the account? | JSIG AC-7 |  |  |  |  |
| 15 | Do all IS display the current DoD Notice and Consent Banner, retain the message until the user acknowledges the usage conditions, and take explicit actions to log on to, or further access, the information system? | JSIG AC-8 |  |  |  |  |
| 16 | Do all SAP IS implement a screen lock within **15 minutes** of user inactivity or upon initiation by the user? | JSIG AC-11 |  |  |  |  |
| 17 | Is a password required for reentry into the system following the session being locked? | JSIG AC-11 |  |  |  |  |
| 18 | When activated, does the session lock place an unclassified pattern onto the display? | JSIG AC-11(1) |  |  |  |  |
| 19 | Are usage restrictions/requirements documented for wireless access? | JSIG AC-18 |  |  |  |  |
| 20 | If allowed, are all wireless access methods documented and approved by the AO? | JSIG AC-18 |  |  |  |  |
| 21 | Does the organization monitor for unauthorized wireless access points/connections? | JSIG SI-4 |  |  |  |  |
| 22 | Are usage restrictions/requirements documented for mobile devices? | JSIG AC-19 |  |  |  |  |
| 23 | If allowed, are mobile devices documented and approved by the AO? | JSIG AC-19 |  |  |  |  |
|  |  |  |  |  |  |  |
| **AWARENESS AND TRAINING** | | | | | | |
| 24 | Is Privileged User training provided to users assigned to positions requiring privileged access before authorizing access to SAP IS, prior to performing assigned duties, when required by system changes, and **at least annually** thereafter? | JSIG AT-3; JSIG PL-4 |  |  |  |  |
| 25 | Are all personnel performing privileged user functions (e.g., security audits, system/network administration, database administration, DTA, etc.) current on training and certification(s) applicable for the position they hold? | DoD 8570.1-M or replacement; JSIG AT-3; JSIG AT-4 |  |  |  |  |
| **AUDIT AND ACCOUNTABILITY** | | | | | | |
| 26 | If automated audit collection is not supported, is use of manual audits documented in the SSP and approved by the AO? | JSIG AU-1 |  |  |  |  |
| 27 | Are all SAP IS configured to audit the events specified **in AU-2** of the JSIG? | JSIG AU-2 |  |  |  |  |
| 28 | Are all SAP IS configured to capture the following content, at a minimum, for each audited event: (1)User ID (2)Type of event/action (3)Success or failure of event/action (4)Date (5)Time (6)Terminal or workstation ID (7)Entity that initiated event/action (8)Entity that completed event/action (9)Remote Access | JSIG AU-3 |  |  |  |  |
| 29 | Is auditing configured and audit record storage capacity allocated to reduce the likelihood of such capacity being exceeded? | JSIG AU-4 |  |  |  |  |
| 30 | (1) Are the audit logs/reports (manual and automated) reviewed **at least weekly**, or at a frequency approved in the SSP? | JSIG AU-6 |  |  |  |  |
| (2) Are the results of these reviews documented in either an electronic or manual log? | JSIG AU-6 |  |  |  |  |
| 31 | Does the IS use an internal system clock for audit time stamps, and are all clocks accurate to within one minute? | JSIG AU-8 |  |  |  |  |
| 32 | Does the SAP IS protect audit information and audit tools from unauthorized access, modification and deletion? | JSIG AU-9 |  |  |  |  |
| 33 | Does the organization limit access to audit functionality to only a small subset of privileged users? | JSIG AU-9(4) |  |  |  |  |
| 34 | Are audit records retained for **a minimum of five (5) years** for SAP information? (The AO has the authority to scale back the retention period depending on the mission of the IS. Such relief must be documented in writing). | JSIG AU-11 |  |  |  |  |
|  |  |  |  |  |  |  |
| **SECURITY ASSESSMENT AND AUTHORIZATION** | | | | | | |
| 35 | Are all connections of an IS to an external IS documented in the SSP and authorized through an ISA, if applicable? | JSIG CA-3 |  |  |  |  |
| 36 | Have all IS POA&Ms been updated **at least quarterly** by the ISO and/or delegate (e.g., ISSM/ISSO)? | JSIG CA-5 |  |  |  |  |
| 37 | Is a current ATO and security authorization package available including, at a minimum: a signed version of the SSP, SAR, RAR, and POA&M? | JSIG CA-6 |  |  |  |  |
| 38 | Does the organization monitor the security controls of all IS on an ongoing basis? (Continuous Monitoring). | JSIG CA-7 |  |  |  |  |
| 39 | Have continuous monitoring reports been provided to the AO/DAO **at least annually**? | JSIG CA-7 |  |  |  |  |
|  |  |  |  |  |  |  |
| **CONFIGURATION MANAGEMENT** | | | | | | |
| 40 | Does the software baseline configuration (e.g., SSP S/W list to include version or release numbers) accurately reflect the current IS? | JSIG CM-2; JSIG CM-7(5) |  |  |  |  |
| 41 | Does the hardware baseline configuration (e.g., SSP H/W list) accurately reflect the current IS to include any laptops, test equipment, projectors, cameras, mobile and other peripheral devices within the authorization boundary? | JSIG CM-2 CM-8 |  |  |  |  |
| 42 | Does the H/W List contain as a minimum: Type, Make, Model, Quantity, Serial Number, Memory (Y/N) and Memory Type, as well as Location? | JSIG CM-8 |  |  |  |  |
| 43 | Does the ISSM/ISSO ensure S/W and H/W changes are tested, validated, documented, and approved by the AO/DAO (as required) prior to implementing on the system? | JSIG CM-3;  JSIG CM-4 |  |  |  |  |
| 44 | Do all IS conform to security configuration/hardening guidance (e.g., lockdown, hardening, security guides, security technical implementation guides (STIGs), or benchmarks) prior to being introduced into a production environment? Are deviations from the guidance documented and justified? | JSIG CM-6 |  |  |  |  |
| 45 | Does the organization monitor, control and document changes to the configuration settings? | JSIG CM-6 |  |  |  |  |
| 46 | Has the IS been configured to provide only essential capabilities and allow only the necessary ports, protocols, and services and reviewed **at least annually** to identify and eliminate unnecessary PPSs? | JSIG CM-7;  JSIG CM 7(1) |  |  |  |  |
| 47 | Has the IS been configured to disable the capability for automatic execution of code (e.g., AutoRun/AutoPlay)? | JSIG CM-7 |  |  |  |  |
| 48 | Does the ISSM ensure all additions, changes or modifications to hardware, software, or firmware are coordinated, via the SCA, with the AO/DAO and are reported within the continuous monitoring program? | JSIG CA-7; JSIG CM-3 |  |  |  |  |
|  |  |  |  |  |  |  |
| **CONTINGENCY PLANNING** | | | | | | |
| 49 | Are backups conducted at least **weekly**, and do they include both user and system-level data? | JSIG CP-9 |  |  |  |  |
| 50 | Is backup information protected to ensure its confidentiality and integrity? | JSIG CP-9 |  |  |  |  |
| 51 | Have procedures to provide for recovery and reconstitution of the IS to a known state following a disruption, compromise or failure been documented and included in the ISCP or SSP? | JSIG CP-10 |  |  |  |  |
|  |  |  |  |  |  |  |
| **IDENTIFICATION AND AUTHENTICATION** | | | | | | |
| 52 | Does the IS uniquely identify and authenticate all users (or processes acting on behalf of users)? | JSIG IA-2 |  |  |  |  |
| 53 | Does the IS uniquely identify and authenticate **all types of devices** before establishing a connection (e.g., servers, workstations, multi-function devices, printers, routers, scanners, VoIP & VTC devices, etc.)? | JSIG IA-3 |  |  |  |  |
| 54 | Are all authenticators (e.g., passwords, PINs, smart cards, tokens, PKI private certificates) protected commensurate with the information sensitivity accessible by the associated entity? | JSIG PL-4 |  |  |  |  |
| 55 | Is the reuse of user, group and device identifiers prevented for **the life of the system**? | JSIG IA-4 |  |  |  |  |
| 56 | Do passwords comply with the IA-5(1) requirements for complexity, number of characters, minimum and maximum lifetime restrictions, and minimum password generations/history before reuse? | JSIG IA-5(1) |  |  |  |  |
| 57 | Are any unencrypted (clear text) passwords stored or transmitted on/by the system, embedded into applications or access scripts, or stored on function keys? | JSIG IA-5(1)(c); JSIG IA-5(7) |  |  |  |  |
|  |  |  |  |  |  |  |
| **INCIDENT HANDLING** | | | | | | |
| 58 | Does the organization test and/or exercise the incident response capability for the IS to determine the incident response effectiveness and document the results? If there were no incidents, are simulated incidents used? | JSIG IR-3 |  |  |  |  |
| 59 | Are all incidents and events (potential or actual) documented and reported **immediately** via secure communicationsto the cognizant PSO and to the AO/DAO **within 24 hours**? | JSIG IR-6 |  |  |  |  |
| 60 | Are copies of the incident response plan distributed to all personnel with a role or responsibility for implementing the plan? | JSIG IR-8 |  |  |  |  |
|  |  |  |  |  |  |  |
| **MAINTENANCE** | | | | | | |
| 61 | Has the organization established a process for authorizing personnel (both cleared and uncleared) to conduct maintenance on the IS? | JSIG MA-5 |  |  |  |  |
| 62 | If appropriately cleared personnel are unavailable to perform maintenance, does the organization provide a fully cleared and technically qualified escort to monitor and record their activities in a maintenance log? | JSIG MA-5 |  |  |  |  |
| 63 | Does the organization record all IS repairs and maintenance activity in a maintenance log for the life of the IS and maintain the log for a minimum of one (1) year after equipment decommissioning or disposal? | JSIG MA-2 |  |  |  |  |
| 64 | Are all off-site maintenance activities specifically authorized prior to the off-site maintenance being performed? | JSIG MA-2 |  |  |  |  |
| 65 | Are all devices sanitized prior to off-site maintenance? | JSIG MA-2 |  |  |  |  |
| 66 | Is the IS checked to verify all controls are still functioning properly following any/all maintenance activities? | JSIG MA-2 |  |  |  |  |
| **MEDIA PROTECTION** | | | | | | |
| 67 | Does the organization sanitize/reuse/dispose of SAP IT components and devices IAW the JSIG and current SAPCO guidance? | JSIG MP-6;  DoD SAPCO Disposition Memo, dtd 27 July 2017 |  |  |  |  |
| 68 | Is all media protected using encryption during transport outside controlled areas? | JSIG MP-5 |  |  |  |  |
|  |  |  |  |  |  |  |
| **PHYSICAL AND ENVIRONMENTAL PROTECTION** | | | | | | |
| 69 | Do all KVM switches comply with the requirements specified in PE-5 overprint in the JSIG? | JSIG PE-5 |  |  |  |  |
| 70 | Are all exceptions to KVM requirements approved by the AO or designee? | JSIG PE-5 |  |  |  |  |
|  |  |  |  |  |  |  |
| **PLANNING** | | | | | | |
| 71 | (1) Is each SSP reviewed **at least annually** and updatedas follows: (2) When hardware/software configuration changes occur? (3) When the system is relocated? (4) When the security categorization changes? (5) When connected to additional networks? | JSIG PL-2 |  |  |  |  |
|  |  |  |  |  |  |  |
| **PERSONNEL SECURITY** | | | | | | |
| 72 | Does the organization ensure that every user accessing SAP IS processing, storing, or transmitting classified information is cleared and indoctrinated for the highest classification and for all of the relevant types of information to which they have access on the system? | JSIG PS-3 |  |  |  |  |
| 73 | Does the organization disable, upon employment termination, information system access within, **if voluntary: as soon as possible, not to exceed 5 working days?** **If involuntary: within same day as termination**? | JSIG PS-4 |  |  |  |  |
| 74 | Does the organization retain all signed User (System) Access Agreements for a minimum of two (2) years after access is removed? | JSIG PS-6 |  |  |  |  |
|  |  |  |  |  |  |  |
| **RISK ASSESSMENT** | | | | | | |
| 75 | Does the organization scan for vulnerabilities in the information system and hosted applications using AO-approved assessment tools **at least quarterly** and when new vulnerabilities potentially affecting the system/applications are identified and reported? | JSIG RA-5 |  |  |  |  |
| 76 | Does the ISSM/ISSO ensure all vulnerability scan reports are analyzed to determine whether reported vulnerabilities apply to the IS (i.e., are the vulnerabilities validated as applicable or false positives)? | JSIG RA-5 |  |  |  |  |
|  |  |  |  |  |  |  |
| **SYSTEM AND COMMUNICATIONS PROTECTION** | | | | | | |
| 77 | Does the organization protect against unauthorized physical connections? | JSIG SC-7(14) |  |  |  |  |
| 78 | Does the IS utilize PDS or encryption during transmission external to the approved space? | JSIG SC-8(1) |  |  |  |  |
| 79 | Are all collaborative computing devices used IAW the requirements documented in the JSIG SC-15 (e.g. no remote activation, explicit indication of use, etc.)? | JSIG SC-15 |  |  |  |  |
| 80 | Does the organization authorize, monitor, and control the use of mobile code within the information system? | JSIG SC-18 |  |  |  |  |
|  |  |  |  |  |  |  |
| **SYSTEM AND INFORMATION INTEGRITY** | | | | | | |
| 81 | Does the organization identify, report, and correct information system flaws? | JSIG SI-2 |  |  |  |  |
| 82 | Does the organization test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation? | JSIG SI-2 |  |  |  |  |
| 83 | Does the organization install security-relevant software and firmware updates **within thirty (30) days** of the release of the updates? | JSIG SI-2 |  |  |  |  |
| 84 | Does the organization employ malicious code protection mechanisms at information system entry and exit points (e.g., firewalls, mail servers, web servers, proxy servers, remote-access servers, workstations, laptops, and mobile devices) to detect and eradicate malicious code? | JSIG SI-3 |  |  |  |  |
| 85 | Does the organization update malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures or every thirty (30) days as a minimum? | JSIG SI-3 |  |  |  |  |
| 86 | Does the organization configure malicious code protection mechanisms to perform periodic scans of the information system **at least weekly** and real-time scans of files from external sources at **endpoints and network entry/exit points** as the files are downloaded, opened, or executed in accordance with organizational security policy? | JSIG SI-3 |  |  |  |  |
| 87 | Does the organization configure malicious code protection mechanisms to **block and quarantine malicious code then send an alert to the system administrator**? | JSIG SI-3 |  |  |  |  |
| 88 | Is each IS that uses removable media configured to automatically scan the removable media for malicious code? If the IS cannot be configured to automatically scan removable media for malicious code, is a user initiated scan conducted? | JSIG SI-3 |  |  |  |  |
| 89 | If the IS is not capable of scanning removable media for malicious code, is the removable media scanned on a separate IS? | JSIG SI-3 |  |  |  |  |
| 90 | Is the SAP IS monitored for unauthorized connections? | JSIG SI-4 |  |  |  |  |
|  |  |  |  |  |  |  |
| **NON-TAILORABLE [SAP TAILORED-IN] CONTROLS**  **For Non-Tailorable controls if “No” then indicate in the remarks if the Senior AO for the system has endorsed a waiver** | | | | | | |
| 91 | Is access to all **IS endpoints (e.g., I/O ports)** explicitly authorized (such as access to USB ports, CD/DVD drives, microphones, and cameras as well as least privilege on ability to make changes to port security implemented on switches)? | JSIG AC-6(1) |  |  |  |  |
| (1) Do all IS technically enforce restrictions on the ability to write to removable media? | JSIG AC-6(1) |  |  |  |  |
| (2) By default, is all write functionality disabled? | JSIG AC-6(1) |  |  |  |  |
| (3) Do all IS audit access (read and write) to removable media? (4) Do all IS log when the write functionality is enabled? And, after the write functions are completed, do all IS log when the write functionality is again disabled? | JSIG AC-6(1); JSIG AU-2.a |  |  |  |  |
| 92 | Does the organization replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer? And for those components with mission/business needs that require their continued use does the organization document justification and approval from the AO? | JSIG SA-22 |  |  |  |  |
| 93 | Do all IS protect the confidentiality of all SAP information at rest through the use of encryption (i.e., DAR encryption)? | JSIG SC-28 |  |  |  |  |