Classified Information System Check Sheet

DATE: \_\_\_\_\_\_\_\_ BLDG: \_\_\_\_\_\_\_ ROOM: \_\_\_\_\_\_\_\_\_\_ CUBE: \_\_\_\_\_\_\_\_\_ ISSO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

SYSTEM NAME: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ SYSTEM NUMBER: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

IS USER(S): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

CLASSIFICATION LEVEL: Confidential Secret Top Secret SAP/SAR

CAVEATS: NATO CNWDI RD/FRD CRYPTO FGI

Administrative

1. The system binder has the ATO letter present with an expiration date that has not elapsed.
2. The system binder has the current DD-254(s) for the program(s) being executed.
3. All user account forms have Program Manager endorsement, CPSO clearance verification, and evidence of need-to-know (re)validation within the last year.
4. All privileged user account forms also have a privileged user acknowledgement form signed by the user.
5. The Audit Review Log is present and has a completed date each week indicating weekly audit was conducted.
6. The BIOS password and emergency administrator account password are recorded and stored in a GSA approved safe.
7. The POA&M is present and properly portion marked and properly stored in a GSA container when classified.
8. The continuous monitoring log is present and up to date. Any gaps or incomplete checks have an accompanying MFR or maintenance log entry.

Information System(s)

1. The BIOS is password protected: The BIOS setting menu shows a lock symbol and cannot be unlocked with a blank password.
2. The BIOS boot order is secure: The information system’s internal hard drive should be the first item in the boot order. There should be no CD, USB, or PXE boot selected.
3. The BIOS has all wireless disabled: If applicable, any wireless options in the BIOS are disabled or not selected.
4. The information system displays the DCSA approved login banner: Refer to DAAPM Appendix X for correct banner.
5. The screen lock is set and enforces screen lock at 15 minutes: Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options >> "Interactive logon: Machine inactivity limit" to "900" seconds".
6. The information system locks user accounts after 3 failed login attempts: Configuration >> Windows Settings >> Security Settings >> Account Policies >> Account Lockout Policy >> "Account lockout threshold" to "3" & "Account lockout duration" to "0" & "Reset account lockout counter after" to "15".
7. SCAP Compliance Checker scan was run within the last 30 days and the score is at least above 90%.
8. User accounts that have not logged in within the last 90 days have been disabled: Review active user accounts and look at last login date. This can be accomplished with an ISSO script that shows all login activity. Review the last login column.
9. All active user accounts have a valid user account form in the system binder as well as a valid privilege user account form if they are a privileged user: Review Computer Management >> Users and Groups. Review all non-disabled (active) user accounts.
10. All privileged user accounts have a general user account as well: Review Computer Management >> Users and Groups. Each active user account in the administrator’s group should have a general user account in the user’s group as well. The general user account for each administrator account does not have to be active, just present.
11. The information system’s anti-malware (anti-virus) definitions have been updated within the last 30 days: Right click Symantec Endpoint Protection icon on the task bar then choose to open. Definition date will be displayed.
12. The information system’s security log is set to not overwrite audit events: Computer Management >> Event Viewer >> Security Log >> Properties “Do not overwrite” is selected.
13. Only authorized users have access to the audit log directories: Go to folder C:\Windows\System32\winevt\Logs. Select Properties >> Security for the Application.evtx, Security.evtx, and System.evtx and verify there are no users with any permissions. Only EIT and ISSOs should have permissions on these files.
14. Only authorized users have access to security relevant objects: Go to folder C:\Security. Select Properties >> Security for the top-level folder and ensure that only EIT and ISSO’s have access to this directory and subfolders.
15. The information system enforces passwords IAW DAAPM Appendix A control IA-5(1): Computer Configuration >> Windows Settings >> Security Settings >> Account Policies >> Password Policy >> "Enforce password history" to "24" & "Maximum Password Age" to "60" & "Minimum Password Age" to at least "1" & "Minimum password length" to "14" & "Password must meet complexity requirements" to "Enabled" & "Store passwords using reversible encryption" to "Disabled".
16. All user accounts have a password required and are not set to never expire: Review ISSO script for user accounts. Verify that password required and password expiration columns do not have users out of compliance.
17. The information system’s patches are current and up to date: Start >> Control Panel >> Programs >> Uninstall a Program >> View Installed Updates. Review “Installed on” column and verify patches have been installed in the last calendar month at a minimum.

**Inspection Team: PRINT NAME SIGNATURE**

Inspector: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsible ISSO:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Responsible ISSM:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

NOTES: