Certification review procedure for standalone systems or peer-to-peer networks with Windows NT, 2000, and XP

<u>Instructions:</u>

- Complete each of the following steps.
- "No" responses indicate that the system <u>does not implement the requisite technical protective measure</u> necessary to meet the requirement, and therefore <u>cannot be certified</u> unless alternative protection measures (variances from protection measures) are documented and tested.
- Document approved variances from technical protective measures and certification procedures, including pass/fail criteria at the end of this form.

⇒ *Step 21 requires information from the SSP. Review the SSP to complete the table in step 21 prior to the certification review.*

⇒ *Read step 20 before proceeding.*

⇒ *This procedure requires the administrator that is conducting the test to know the Administrator password.*

1. Ask an administrator to boot the system, pressing the key(s) required to activate the BIOS configuration (hold down the Delete or F1 key while booting).

   Did the system require a password to enter the BIOS configuration program? (NISPOM 8-613.a(1)) □ Yes □ No

   Ask the administrator to navigate through the BIOS configuration. Look for control settings for wireless communications devices, such as infrared and radio frequency wireless communications, including Bluetooth.

   Are all wireless communications devices disabled in the BIOS, or have the physical transmission interfaces been physically disabled or removed? (NISPOM 8-605.a) □ Yes □ No

   Ask the administrator to insert formatted media into all removable media devices on the system. Ask the administrator to exit the BIOS configuration menu and resume booting the system.

   Did the system boot from the hard drive? (If the system displayed an error message indicating a non-system disk, then it was trying to boot from the removable media instead of the hard drive.) (NISPOM 8-613.a(1)) □ Yes □ No

   Ask the administrator to remove the removable media and resume booting the system if necessary.

2. Ask an administrator to log in on an account that is a member of the Administrators group.

   Is the warning banner displayed by the system? (NISPOM 8-609.a(1)) □ Yes □ No
   Is the warning banner the approved version? □ Yes □ No
   Record the approximate time from the clock in the system tray. ______________________________ 528
   Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

   Some systems may be configured to meet corporate security policy settings as well as NISPOM settings. For this certification review, the following local security policy settings are required. If the system is configured other than as required for this test, record the current settings before changing them to meet the requirements for the test.

   - *Control Panel* ➔ *Administrative Tools* ➔ *Local Security Policy* ➔ *Security Settings* ➔ *Account Policies* ➔ *Password Policy* ➔ *Minimum password age* must be set to 0. Present setting: ________

3. Ask the administrator to create a new user account using *Control Panel* ➔ *Administrative Tools* ➔ *Computer Management* for a general user, configure the account as required in the SSP for a general user. Ask the administrator to leave the password field blank when the account is created, i.e., attempt to create an account without a password.

   Did the system prevent the account with no password from being created? (NISPOM 8-303.b) □ Yes □ No

   Ask the administrator to assign a valid password for the account, and finish creating the account. Ask the administrator to close computer management.

4. Ask the administrator to create a second new user account using *Control Panel* ➔ *User Accounts* or *Control Panel* ➔ *Users & Passwords* for a general user, configure the account as required in the SSP for a general user. Ask the administrator to leave the password field blank when the account is created, i.e., attempt to create an account without a password.

   Did the system prevent the use of this method to create user accounts? (NISPOM 8-303.b) □ Yes □ No

   If the system prevented the account with no password from being created, skip over the rest of this step, and proceed with step 4. Otherwise, continue the procedures in this step.

   Did the system prevent the account with no password from being created?[**] (NISPOM 8-303.b) □ Yes □ No

   If the system prevented the account with no password from being created, skip over the rest of this step, and proceed with step 4. Otherwise, continue the procedures in this step.

Ask the administrator to log out.

Record the approximate time from the clock in the system tray. ______________________________ *538
*May be event type 551 on Windows XP/Pro
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

Ask the administrator to attempt to log on as the <u>second</u> new user, providing no password at the prompt.

Did the system prevent log on to the account with no password? (NISPOM 8-303.b) □ Yes □ No

** If the system prevented the log on to the account with no password, then a "No" response to this question is acceptable.

If the administrator logged on successfully, then ask the administrator to log off as the second new user, and then log in on an account that is a member of the Administrator's group.

Ask the administrator to delete the second new user account and log out.

Record the approximate time from the clock in the system tray. ______________________________ *538
*May be event type 551 on Windows XP/Pro
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

5. Ask the administrator to log in to the new user account that was just created. (You should see the warning banner again in case you missed it earlier.)

   Record the approximate time from the clock in the system tray. ______________________________ 528
   Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

6. Ask the administrator, as the new user, to change the password to a complex seven character password, such as "!wH8p?x".

   Did the system prevent the change? (NISPOM 8-303.i(2)) □ Yes □ No

7. Ask the administrator, as the new user, to change the password to a simple password, such as "security".

   Did the system prevent the change? (NISPOM 8-303.i(3)) □ Yes □ No

8. Ask the administrator, as the new user, to change the password to an acceptable password, "Go2UrHome".

Record the approximate time from the clock in the system tray. ________________________________ 627
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(d)) □ Yes □ No

9. Ask the administrator, as the new user, to change the password to the current password to the same password. That is, change the password by entering the current password, "Go2UrHome" in the old password field, and then enter the same password in the new password field.

   Did the system prevent the change? (NISPOM 8-303.i) □ Yes □ No

10. Ask the administrator, as the new user, to open "My Computer", then C:\WINNT (C:\WINDOWS on XP/Pro). Open any text file in the C:\WINNT directory (C:\WINDOWS on XP/Pro). Modify the file. Ask the administrator to save the file in the C:\WINNT directory.

    Did the system prevent the general user from saving the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
    Record the approximate time from the clock in the system tray. ________________________________ 560
    Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

    Ask the administrator, as the new user, to save the file under a different name in the same directory (C:\WINNT).

    Did the system prevent the general user from saving the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
    Record the approximate time from the clock in the system tray. ________________________________ 560
    Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

11. Ask the administrator, as the new user, to open the event viewer. Attempt to view the security log.

    Did the system prevent the general user from opening the security event log? (NISPOM 8-602.a(2)) □ Yes □ No
    Record the approximate time from the clock in the system tray. ________________________________ 560
    Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

    In Explorer, open the directory C:\WINNT\SYSTEM32\config (or the alternate location where the system stores the audit logs). Attempt to delete the security event log, SecEvent.evt.

    Did the system prevent the general user from deleting the file? (NISPOM 8-602.a(2)) □ Yes □ No
    Record the approximate time from the clock in the system tray. ________________________________ 560
    Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

12. Ask the administrator, as the new user, to try to copy the SAM file to his desktop. If successful, be sure to delete the file from the desktop and empty the wastebasket.

Did the system prevent the general user from accessing the file? (NISPOM 8-303.d) □ Yes □ No
Record the approximate time from the clock in the system tray. ______________________ 560
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

13. Ask the administrator, as the new user, to change the system clock.

Did the system prevent the general user from changing the clock? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
Record the approximate time from the clock in the system tray. ______________________ 560
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

14. Ask the administrator, as the new user, to turn off the real time virus protection.

Did the system prevent the general user from disabling virus protection? (NISPOM 8-305, 8-307, 8-613.a(1)) □ Yes □ No
Record the approximate time from the clock in the system tray. ______________________
Was the event recorded in any log? (Most anti-virus products will not log.) (NISPOM 8-602.a(1)(c)) □ Yes □ No

15. Ask the administrator to identify all remaining security relevant programs on the system, and their installation directories. Ask the administrator, as the new user, to open Notepad, and enter a random meaningless data stream, such as "asdf", into the file. For each security relevant program, ask the administrator to attempt to save the Notepad file as the security relevant program.

□ Hex editor Location: ______________________________
Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
Record the approximate time from the clock in the system tray. ______________________ 560
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

□ Overwriting software Location: ______________________________
Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
Record the approximate time from the clock in the system tray. ______________________ 560
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

□ Dirty word search Location: ______________________________
Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
Record the approximate time from the clock in the system tray. ______________________ 560
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

□ Password generator Location: ____

Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No

Record the approximate time from the clock in the system tray. ______________________________ 560

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

□ Alternate location for audit logs Location: ____

Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No

Record the approximate time from the clock in the system tray. ______________________________ 560

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

□ Other: ____________________ Location: ____

Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No

Record the approximate time from the clock in the system tray. ______________________________ 560

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

□ Other: ____________________ Location: ____

Did the system prevent the general user from replacing the file? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No

Record the approximate time from the clock in the system tray. ______________________________ 560

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(c)) □ Yes □ No

16. Ask the administrator, as the new user, to log off.

Record the approximate time from the clock in the system tray. ______________________________ *538

*May be event type 551 on Windows XP/Pro

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

17. Ask the administrator to attempt to logon to the Guest account, providing no password.

Did the logon fail? (NISPOM) □ Yes □ No

Record the approximate time from the clock in the system tray. ______________________________ 531

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

18. Ask the administrator to attempt to logon to the new user account, using the wrong password.

Did the logon fail? (NISPOM) □ Yes □ No

Record the approximate time. ______________________________ 529

Was the event recorded in the security event log? (NISPOM 8-602.a(1)(b)) □ Yes □ No

19. Repeat the previous step a maximum of 4 times for a total of 5 unsuccessful logon attempts on the new user ID.

Was the user ID disabled? (NISPOM 8-609.a(2)(a)) □ Yes □ No
Record the approximate time. ______________________ 539
Was the event recorded in the security event log? (NISPOM 8-602.a(1)(f)) □ Yes □ No

20. Ask the administrator to log in on an account that is a member of the Administrators group. Open the security event log. Review the security event log for entries created by procedures above that include recording the time and that contain a question asking whether a log entry was made. The number following the blank where the time was recorded is the event type that will appear in the security event log. Check the appropriate box.

21. Review the SSP to identify the classes of user privileges (Users, Power Users, Backup Operators, Administrators, etc., or as defined in the SSP). Record the classes.

User privileges

□ General user (Users)	□ Administrators	□
□	□	□
□	□	□

Ask the administrator to open the user and group manager. Review the membership of each group.

Are general user accounts, including the test account, identified as members of the "Users" group only? (NISPOM 8-307, 8-613.a(1)) □ Yes □ No
Do the privileged accounts identified in the user privileges table above match the privileged groups identified in the group manager on the system? (NISPOM 8-307) □ Yes □ No
Are privileged users assigned to the proper privileged groups? (NISPOM 8-613.a) □ Yes □ No

22. Ask the administrator to open the property sheet for the anti virus software (right click on the anti virus icon in the system tray, select "Properties" or "About").

Are the anti virus signatures (virus definitions) current? (NISPOM 8-305) □ Yes □ No

23. Ask the administrator to set the system time ahead by 13 months, and then log out from the administrative account. Ask the administrator to log in on the new user account.

    Did the system require the selection of a new password? (NISPOM 8-303.i(2)) □ Yes □ No

    Ask the administrator to complete the log in by selecting a new password. Ask the administrator to log off, then log in on the Administrator account.

    Did the system prompt the Administrator to select a new password? (NISPOM 8-303.i(2)) □ Yes □ No

    Ask the administrator to cancel the box prompting for the selection of a new password.

    Did the system prevent the Administrator from proceeding without selection of a new password? (NISPOM 8-303.i(2)) □ Yes □ No

    Ask the administrator to open the user management console, *Control Panel ➔ Administrative Tools ➔ Computer Management ➔ Local Users and Groups ➔ Users*. Review the properties for each user, noting the setting for "Password never expires".

    Do ***all*** accounts have the "Password never expires" box *unchecked*? (NISPOM 8-303.i(2)) □ Yes □ No

    Ask the administrator to reset the system clock to the correct time, and to remove the new user account.

Restore local policy settings that were modified during step 2. □ **Complete**

24. Document variance(s) from technical protection measures, the certification test procedure, and the pass/fail criteria.

Variance:	NISPOM paragraph(s):
Test procedure:	□ Yes/Pass □ No/Fail
Variance:	NISPOM paragraph(s):
Test procedure:	□ Yes/Pass □ No/Fail
Variance:	NISPOM paragraph(s):
Test procedure:	□ Yes/Pass □ No/Fail