# Compliance Self Test Plan for GENERIC, Windows 7 OS, version 2016

## 09 NOV 2023

# SIGNATURES

**Information System Security Manager:**

________________________________________ ________________

**Name** **Date**

**ISSM**

**Information System Security Officer:**

________________________________________ ________________

**Name** **Date**

**ISSO**

TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1 Purpose

The purpose of the GENERIC Test Plan is to provide all involved parties with a discrete set of measurement and expected outcomes in order to gauge successful security compliance self-testing for the GENERIC system at the installation location.  Additionally, this document will outline the resources needed to successfully accomplish this test.

## 1.2 Scope

The scope of this test includes the test cases for the Windows 7 operating system on the GENERIC baseline system.

## 2. Environment (Target System)

The GENERIC system is comprised of the following sub-systems with associated operating systems and Original Equipment Manufacturer (OEM) as defined;

- INSERT SYSTEM (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER]

- LIST

The interface control systems that are testable in the target system include the account consoles to the GENERIC system, as defined by access through the sub-system.

### 2.1 Security Environment

The security environment will be at the [INSERT LEVEL OF SECURITY] level and will require the appropriate security and control measures suitable for the data being processed. All personnel will require access authorization to both the testing facility and the data produced on the system components. Any test materials, data, or reports identified as being classified will require the appropriate markings, protection, transmission, handling and storage procedures.

# 3. Responsibilities

## 3.1 Site ISSM

Organizational personnel will provide logistical and technical support to the OEM team during the installation and test period. Support should include any system administration or network administration that must be accomplished on the host environment in order to successfully integrate the test system into the [ORGANIZATIONAL] network.

## 3.2 Site ISSO

Implementation of appropriate security controls to maintain information system risk and associated mission risk at an acceptable level as determined by the Authorizing Authority (AO). The system controls, the particular controls with [ORGANIZATIONAL] defined parameters in Committee on National Security Systems Instruction (CNSSI) 1253 are referenced by the following list:

- INSERT SYSTEM CONTROL (ABBREVIATION) [OPERATING SYSTEM, ORGANIZATION OWNER] [PARAMETER]

- LIST

## 3.3 [ORGANIZATION]

Develop the cyber security compliance self-test plan. The test procedures contained in this document are referenced to 2016 values for Windows 7 Operating System.

## 4. Test Execution Instructions

i) The test procedure sheet may be filled out manually or electronically.
   (1) Complete the entries for target system, date, and test representative at the beginning of the procedure.
   (2) All information assurance security controls in the table must be marked as:
      (a) Pass:
         (i) the device passed the security test
      (b) Fail:
         (i) the device failed the test; or
         (ii) device lacks the capability and is not compensated by another device/measure
      (c) Not Evaluated:
         (i) no test provided; or
         (ii) the device is not available for testing; or
         (iii) the device lacks the capability but is compensated by another device/measure
   (3) Provide comments for any control not marked as Pass.
   (4) Upon completion, the score sheet is digitized if necessary, and uploaded as an exhibit to the appropriate [ORGANIZATION] project reference.

### 4.1 Test Procedure

The following pages provide the detailed test procedure required to perform the target system compliance self-test plan.

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Security Test Case**<br>TEST SCENARIO:<br>The test executioner will log onto a [access interface] workstation and execute a series of commands and check the results against the respective expected results that are listed below.<br>TEST SETUP:<br>1. The test executioner will log into a [access interface] workstation with valid LDAP user with privileged access (account should have a ".priv" at the end of it).<br>2. Once logged on, the test executioner will open a shell by clicking on Hosts and selecting Console.<br>3. Within the shell, the test execution will execute the following shell commands | | | |
| N/A | **Record Test Start Date/Time** | **Start Date: _______ Start Time: ________** | N/A |
| **Test 1 AC-2 (1) Account Management: The organization employs automated mechanisms to support the management of information system accounts. NSS Defined Value [], AF Defined Value []** | | | |
| 1 | Select Start->Administrative Tools->Active Directory Users and Computers. Select the Domain and then select the "Users" folder.<br>Adding a user: Right-click the Users folder, then select New/User.<br>Deleting a user: Highlight the user and select the "Delete" key. At the Confirmation window, select "Yes". | Creating/Deleting a user (domain controller) | |
| 2 | Select Start->Computer Management.<br>Select System Tools/Local users and Groups/Users.<br>To Add a user: select Action/New User.<br>Type in the following: Username Full Name Password Confirm Password<br>Deselect "User must change password at next logon."<br>Select the "Create" button to create the user. | Creating a user on a WIN7 Client | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td colspan="4"><b>Test 2 AC-2 (2) Account Management: The information system automatically terminates temporary and emergency accounts after [Assignment: organization-defined time period for each type of account]. NSS Defined Value . . . not to exceed 72 hours., AF Defined Value []</b></td></tr>
<tr><td>3</td><td>Review site account establishment and management processes and interview account managers</td><td>Processes should include:<br>a. Identification of account types (i.e., individual, group, system, application, guest/anonymous, and temporary)<br>b. Establishing conditions for group membership<br>c. Identifying authorized users of the information system and specifying access privileges<br>d. Requiring appropriate approvals for requests to establish accounts<br>e. Establishing, activating, modifying, disabling, and removing accounts<br>f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts<br>g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes<br>h. Deactivating:<br>- temporary accounts that are no longer required<br>- accounts of terminated or transferred users<br>i. Granting access to the system based on:<br>- valid access authorization<br>- intended system usage<br>- other attributes as required by the organization or associated missions/business functions<br>j. Reviewing accounts during some defined frequency</td><td></td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>4</td><td>Verify the operating system automatically disables temporary user accounts after 72 hours.<br>Determine if temporary user accounts are used and identify any that may be in existence.<br>For Domain Accounts:<br>Open PowerShell.<br>Run the command "Search-ADAccount -AccountExpiring" to determine if account expiration dates have been configured on any temporary accounts.<br>For any accounts returned, run the command "Get-ADUser -Identity <Name> -Property WhenCreated" to determine when the account was created.<br>Local accounts:<br>Run "Net user <username>".  This will list the account properties, including "Account Expires".</td><td>Temporary user accounts do not exist.<br>The operating system does not automatically disable emergency accounts.</td><td></td></tr>
<tr><td colspan="4"><b>Test 3 AC-2 (3) Account Management: The information system automatically disables inactive accounts after [Assignment: organization-defined time period]. NSS Defined Value . . . not to exceed 90 days, AF Defined Value []</b></td></tr>
<tr><td>5</td><td>Administrative Tools –<br>Local Security Policy –<br>Security –<br>Account Policy –<br>Password Policy</td><td>Password Parameters</td><td></td></tr>
<tr><td colspan="4"><b>Test 4 AC-2 (4) Account Management: The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. NSS Defined Value [], AF Defined Value []</b></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 6 | Security Option “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” must be set to “Enabled” for the detailed auditing subcategories to be effective.<br>Use the AuditPol tool to review the current Audit Policy configuration:<br>-Open a Command Prompt with elevated privileges (“Run as Administrator”).<br>-Enter “AuditPol /get /category:*”.<br>Compare the Auditpol settings with the expected results. | Account Management -> Security Group Management - Success<br>Account Management -> User Account Management - Success<br>Account Management -> Security Group Management - Failure<br>Account Management -> User Account Management - Failure | |
| **Test 5 AC-2 (7) Account Management: The organization: (a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes information system and network privileges into roles; and (b) Tracks and monitors privileged role assignments. NSS Defined Value [], AF Defined Value []** | | | |
| 7 | Review account establishment and management processes and interview account managers | Procedures should include role-based access schemes and a mechanism for tracking role assignment. | |
| **Test 6 AC-3 Access Enforcement: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy. NSS Defined Value [], AF Defined Value []** | | | |
| 8 | Open the Computer Management Console.<br>Expand "Storage" in the left pane.<br>Select "Disk Management".<br>Some hardware vendors create a small FAT partition to store troubleshooting and recovery data. No other files must be stored here. This must be documented with the ISSO. | the file system column indicates "NTFS" as the file system for each local hard drive | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 9 | Open "Devices and Printers" in Control Panel.<br>If there are no locally attached printers, this is NA.<br>Perform this check for each locally attached printer:<br>Right-click on a locally attached printer.<br>Select "Printer Properties".<br>Select the "Sharing" tab.<br>View whether "Share this printer" is checked.<br>Perform this check on each printer that has the "Share this printer" selected:<br>Select the Security tab. | No non-administrative user accounts or groups have greater than "Print" | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 10 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> User Rights Assignment.<br>Systems dedicated to managing Active Directory (AD admin platforms), must only allow Administrators, removing the Users group.<br>Administrators may be granted this user right if Remote Desktop Services is necessary for remote administration.  Restricted Admin mode must be used.  This must be document with the ISSO.<br>Restricted Admin mode for Remote Desktop Connections can be implemented for each session using a command line switch to start the Remote Desktop Client or through a group policy to enable it for all sessions.<br>The command line to do this is "mstsc /restrictedadmin".<br>To enable this with group policy, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Credentials Delegation >> "Restrict delegation of credentials to remote servers" to "Enabled". | No accounts or groups other than the following are granted the "Access this computer from the network" right: Administrators<br>No accounts or groups other than the following are granted the "Allow log on locally" user right: Administrators, Users<br>No accounts or groups are granted the "Allow log on through Remote Desktop Services" right<br>Administrators may be granted this user right if Remote Desktop Services is necessary for remote administration.  Restricted Admin mode must be used.  This must be document with the ISSO. |  |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 11 | Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> User Rights Assignment. | the following accounts or groups are defined for the "Deny access to this computer from the network" right<br><br>Domain Systems Only:<br>Enterprise Admins group<br>Domain Admins group<br>All Local Administrator Accounts:<br>*Systems with the new built-in security groups - use "Local account" or "Local account and member of Administrators group".<br>**Systems that do not have the new built-in security groups - use the "DenyNetworkAccess" or "DeniedNetworkAccess" group (see V-45589).<br>Do not use the built-in Administrators group.  This group must contain the appropriate accounts/groups responsible for administering the system.<br><br>All Systems:<br>Guests group<br><br>Systems dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups. | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 12 | Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> User Rights Assignment. | the following accounts or groups are defined for the "Deny log on as a batch job" right<br>Domain Systems Only:<br>Enterprise Admins Group<br>Domain Admins Group<br>All Systems:<br>Guests Group<br>the following accounts or groups are defined for the "Deny log on as a service" right on domain joined systems<br>Enterprise Admins Group<br>Domain Admins Group<br>No accounts or groups are defined for the "Deny log on as a service" right on non-domain joined systems | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 13 | Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> User Rights Assignment. | the following accounts or groups are defined for the "Deny log on locally" right<br>Domain Systems Only:<br>Enterprise Admins Group<br>Domain Admins Group<br>Workstations dedicated to the management of Active Directory are exempt from this.<br>the following accounts or groups are defined for the "Deny log on through Remote Desktop Services" right<br>Domain Systems Only:<br>Enterprise Admins group<br>Domain Admins group<br>All Local Administrator Accounts:<br>*Systems with the new built-in security groups - use "Local account" or "Local account and member of Administrators group".<br>**Systems that do not have the new built-in security groups - use the "DenyNetworkAccess" or "DeniedNetworkAccess" group<br>Do not use the built-in Administrators group.  This group must contain the appropriate accounts/groups responsible for administering the system.<br>All Systems:<br>Guests group<br>Systems dedicated to the management of Active Directory are exempt from denying the Enterprise Admins and Domain Admins groups.<br>No accounts or groups are granted the "Log on as a batch job" right<br>No accounts or groups are granted | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 7 AC-3 (4) Access Enforcement: The information system enforces a Discretionary Access Control (DAC) policy that: (a) Allows users to specify and control sharing by named individuals or groups of individuals, or by both; (b) Limits propagation of access rights; and (c) Includes or excludes access to the granularity of a single user. NSS Defined Value [], AF Defined Value []** | | | |
| 14 | Review the discretionary access control, access enforcement policies and procedures | User accounts are role-based. The role assigned to the account defines the user’s access. The policy is bounded by the information system boundary. | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 15 | The default ACL settings are adequate when the Security Option "Network access: Let Everyone permissions apply to anonymous users" is set to "Disabled."<br>Verify the default permissions for the sample directories below. Non-privileged groups such as Users or Authenticated Users must not have greater than Read & execute permissions except where noted as defaults. (Individual accounts must not be used to assign permissions.)<br>Viewing in Windows Explorer:<br>Right click on the directory and select "Properties".<br>Select the "Security" tab, and the "Advanced" button.<br>C:\\<br>Type - "Allow" for all<br>Inherited from - "<not inherited>" for all<br>Name - Permission - Apply to<br>Administrators - Full control - This folder, subfolders and files<br>SYSTEM - Full control - This folder, subfolders and files<br>Users - Read & execute - This folder, subfolders and files<br>Authenticated Users - Special - Subfolders and files only<br>(Special = all permissions except Full Control, Delete subfolders and files, Change permissions, and Take ownership when viewing permission details.)<br>Authenticated Users - Create folders / append data - This folder only<br>The Program Files, Program Files (x86), and Windows directories have the following default permissions:<br>Type - "Allow" for all<br>Inherited from - "<not inherited>" for all | the default ACLs are maintained and the referenced option is set to "Disabled"<br>If a permission setting prevents a site's applications from performing properly, settings must only be changed to the minimum necessary for the application to function. Each exception must be documented with the ISSO. | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| | Name - Permission - Apply to<br>TrustedInstaller - Special - This folder and subfolders<br>(Special = Full control when viewing permission details.)<br>SYSTEM - Special - This folder only<br>(Special = all permissions except Full Control, Delete subfolders and files, Change permissions, and Take ownership when viewing permission details.)<br>SYSTEM - Special - Subfolders and files only<br>(Special = Full control when viewing permission details.)<br>Administrators - Special - This folder only<br>(Special = all permissions except Full Control, Delete subfolders and files, Change permissions, and Take ownership when viewing permission details.)<br>Administrators - Special - Subfolders and files only<br>(Special = Full control when viewing permission details.)<br>Users - Read & execute - This folder, subfolders and files<br>CREATOR OWNER - Special - Subfolders and files only<br>(Special = Full control when viewing permission details.)<br><br>Alternately use Icacls.<br><br>In a Command prompt (admin)<br>Enter icacls followed by the directory.<br><br>icacls c:\\<br>icacls "c:\program files" of "c:\program files (x86)"<br>icacls c:\windows<br><br>The following results will be displayed as each is entered:<br><br>c:\\ | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| | BUILTIN\Administrators:(F)<br>BUILTIN\Administrators:(OI)(CI)(IO)(F)<br>NT AUTHORITY\SYSTEM:(F)<br>NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)<br>BUILTIN\Users:(OI)(CI)(RX)<br>NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(M)<br>NT AUTHORITY\Authenticated Users:(AD)<br>Mandatory Label\High Mandatory Level:(OI)(NP)(IO)(NW)<br>Successfully processed 1 files; Failed processing 0 files<br><br>c:\program files, c:\program files (x86), and c:\windows<br>NT SERVICE\TrustedInstaller:(F)<br>NT SERVICE\TrustedInstaller:(CI)(IO)(F)<br>NT AUTHORITY\SYSTEM:(M)<br>NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)<br>BUILTIN\Administrators:(M)<br>BUILTIN\Administrators:(OI)(CI)(IO)(F)<br>BUILTIN\Users:(RX)<br>BUILTIN\Users:(OI)(CI)(IO)(GR,GE)<br>CREATOR OWNER:(OI)(CI)(IO)(F)<br>Successfully processed 1 files; Failed processing 0 files | | |
| **Test 8 AC-4 Information Flow Enforcement: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy. NSS Defined Value [], AF Defined Value []** | | | |
| 16 | Ask the system administrator if network bridging software is installed on the system or the system is configured for network bridging. | No network bridging software is installed or the system is not configured for network bridging. | |
| 17 | None | Windows 7 does not have Flow Control capabilities | |
| **Test 9 AC-6 Least Privilege: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 18 | Navigate to the following registry key:<br>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.<br>Verify the permissions assigned. | Standard user accounts and groups will only have Read permissions to this registry key. | |
| 19 | Using the Registry Editor, navigate to the following key:<br>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\ | the key exists<br>the permissions are at least as restrictive as those below<br>Administrators - Full<br>Backup Operators - Read(QENR)<br>Local Service - Read | |
| 20 | Review the local Administrators group. Only the appropriate administrator groups or accounts responsible for administration of the system may be members of the group.<br>For domain-joined workstations, the Domain Admins group must be replaced by a domain workstation administrator group.<br>Systems dedicated to the management of Active Directory are exempt from this. AD admin platforms may use the Domain Admins group or a domain administrative group created specifically for AD admin platforms.<br>Standard user accounts must not be members of the local administrator group. | prohibited accounts are not members of the local administrators group | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 21 | Navigate to the following registry key and review the assigned permissions:<br>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components<br>On 64-bit systems also review the permissions assigned to the following registry key:<br>HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components<br>Verify that standard user accounts and groups only have Read permissions to this registry key. | No standard user accounts or groups have greater permissions | |
| 22 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> User Rights Assignment. | No accounts or groups (to include administrators), are granted the "Act as part of the operating system" right<br>No accounts or groups are granted the "Create a token object" right<br>No accounts or groups are granted the “Debug programs” right | |
| **Test 10 AC-7 Unsuccessful Login Attempts: The information system: a. Enforces a limit of [Assignment: organization-defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period; and b. Automatically [Selection: locks the account/node for an [Assignment: organization-defined time period]; locks the account/node until released by an administrator; delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login is done via a local, network, or remote connection. NSS Defined Value a. . . .a maximum of 3 . . .15 minutes b. . . .locks the account/node until unlocked by an administrator, AF Defined Value []** | | | |
| 23 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Account Policies >> Account Lockout Policy. | the "Account lockout threshold" is not "0" or more than "3" attempts<br>the "Reset account lockout counter after" value is not less than "15" minutes<br>the "Account lockout duration" is set to "0", requiring an administrator to unlock the account | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 11 AC-7 (1) Unsuccessful Login Attempts: The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded. NSS Defined Value [], AF Defined Value []** | | | |
| 24 | See AC-7 | See AC-7 | |
| **Test 12 AC-8 System Use Notification: The information system: a. Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a U.S. Government information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 25 | Access the system console and make a logon attempt. Check for either of the following login banners based on the character limitations imposed by the system. An exact match is required. | The following banner is displayed:<br>"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.<br>By using this IS (which includes any device attached to this IS), you consent to the following conditions:<br>-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.<br>-At any time, the USG may inspect and seize data stored on this IS.<br>-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.<br>-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.<br>-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. " | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 26 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options. | the value for “Interactive Logon: Message title for users attempting to log on” is set to “DoD Notice and Consent Banner”, “US Department of Defense Warning Statement”, or a site defined equivalent<br>Automated tools may only search for the titles defined above. If a site defined title is used, a manual review will be required.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \Software\Microsoft\Windows\CurrentVersion\Policies\System\<br>Value Name: LegalNoticeCaption<br>Value Type: REG_SZ<br>Value: See message title above | |
| **Test 13 AC-9 Previous Logon (Access) Notification: The information system notifies the user, upon successful logon (access), of the date and time of the last logon (access). NSS Defined Value [], AF Defined Value []** | | | |
| 27 | From the Login screen, log on to the system as an administrator | A login message displays date and time of the user’s last login | |
| 28 | In Group policy editor, navigate to Computer Configuration -> Policies -> Administrative Templates -> Windows Components -> Windows Logon Options | Display information about previous logons during user logon = Enabled | |
| **Test 14 AC-11 Session Lock: The information system: a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and … b. Retains the session lock until the user reestablishes access using established identification and authentication procedures. NSS Defined Value a. . . .not to exceed 30 minutes, AF Defined Value []** | | | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>29</td><td>Registry Hive: HKEY_CURRENT_USER<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop\<br>Value Name: ScreenSaveActive<br>Value Type: REG_SZ<br>Value: 1<br>Value Name: ScreenSaverIsSecure<br>Value Type: REG_SZ<br>Value: 1<br>Value Name: ScreenSaveTimeout<br>Value Type: REG_SZ<br>Value: 900 (or less)<br>Applications requiring continuous, real-time screen display (e.g., network management products) require the following and must be documented with the ISSO.<br>-The logon session does not have administrator rights.<br>-The display station (e.g., keyboard, monitor, etc.) is located in a controlled access area.</td><td>the registry values do not exist or are configured as step description defines</td><td></td></tr>
<tr><td colspan="4"><b>Test 15 AC-11 (1) Session Lock: The information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>30</td><td>Right-click on desktop, select personalization, then select screen saver.</td><td>Wait box = 30 minutes or less. “on resume, display login screen” setting selected.</td><td></td></tr>
<tr><td colspan="4"><b>Test 16 AC-14 Permitted Actions Without Identification Or Authentication: The organization: a. Identifies specific user actions that can be performed on the information system without identification or authentication; and b. Documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. NSS Defined Value [], AF Defined Value []</b></td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>31</td><td>None</td><td>Users must have an account (username and password) for login access to the SYSTEM application. Administrators must have a privileged account to login to the SYSTEM.</td><td></td></tr>
<tr><td colspan="4"><b>Test 17 AC-14 (1) Permitted Actions Without Identification Or Authentication: The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission/business objectives. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>32</td><td>Review Permitted Actions Without Identification Or Authentication</td><td>identification and authentication only access</td><td></td></tr>
<tr><td colspan="4"><b>Test 18 AC-17 Remote Access: The organization: a. Documents allowed methods of remote access to the information system; b. Establishes usage restrictions and implementation guidance for each allowed remote access method; c. Monitors for unauthorized remote access to the information system; d. Authorizes remote access to the information system prior to connection; and e. Enforces requirements for remote connections to the information system. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>33</td><td>Review remote access authorization policy and procedures.</td><td>Remote access is documented in policy and procedures</td><td></td></tr>
<tr><td colspan="4"><b>Test 19 AC-17 (1) Remote Access: The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods. NSS Defined Value [], AF Defined Value []</b></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 34 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\<br>Value Name: fDenyTSConnections<br>Value Type: REG_DWORD<br>Value: 1<br>If Remote Desktop Services for remote administration is necessary, enabling this is ok. Restricted Admin mode must be used. This must be document with the ISSO.<br>Restricted Admin mode for Remote Desktop Connections can be implemented for each session using a command line switch to start the Remote Desktop Client or through a group policy to enable it for all sessions.<br>The command line to do this is "mstsc /restrictedadmin".<br>To enable this with group policy, configure the policy value for Computer Configuration >> Administrative Templates >> System >> Credentials Delegation >> "Restrict delegation of credentials to remote servers" to "Enabled". | the registry value does exist and is configured as specified | |
| 35 | Security Option “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” must be set to “Enabled” for the detailed auditing subcategories to be effective.<br>Use the AuditPol tool to review the current Audit Policy configuration:<br>-Open a Command Prompt with elevated privileges (“Run as Administrator”).<br>-Enter “AuditPol /get /category:*”. | the system should audit the following:<br>Logon/Logoff -> Logoff - Success<br>Logon/Logoff -> Logon - Success<br>Logon/Logoff -> Logon - Failure | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 20 AC-17 (2) Remote Access: The organization uses cryptography to protect the confidentiality and integrity of remote access sessions. NSS Defined Value [], AF Defined Value []** | | | |
| 36 | Verify encryption is required for remote access. | userid and password information are encrypted<br>administrator data is encrypted<br>user data coming from or going outside the enclave is encrypted | |
| 37 | Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\<br>Value Name: MinEncryptionLevel<br>Type: REG_DWORD<br>Value: 3 | the registry value exists and is configured as specified | |
| **Test 21 AC-17 (3) Remote Access: The information system routes all remote accesses through a limited number of managed access control points. NSS Defined Value [], AF Defined Value []** | | | |
| 38 | None | Access control points are managed by the network enclave. This control is inherited from the network enclave. | |
| **Test 22 AC-17 (4) Remote Access: The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 39 | None | Access control points are managed by the network enclave. This control is inherited from the network enclave. | |
| **Test 23 AC-17 (7) Remote Access: The organization ensures that remote sessions for accessing [Assignment: organization-defined list of security functions and security-relevant information] employ [Assignment: organization-defined additional security measures] and are audited. NSS Defined Value [], AF Defined Value . . .privileged functions and security relevant information . . . Secure Shell [SSH], Virtual Private Networking [VPN]**<br>**. . .other encrypted channel with blocking mode enabled** | | | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>40</td><td>Review remote access policies and procedures</td><td>. . . privileged functions and security relevant information . . . Secure Shell [SSH], Virtual Private Networking [VPN]<br>. . . other encrypted channel with blocking mode enabled</td><td></td></tr>
<tr><td colspan="4"><b>Test 24 AC-18 (1) Wireless Access Restrictions: The information system protects wireless access to the system using authentication and encryption. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>41</td><td>Review remote access authorization policy and procedures.</td><td>No wireless access allowed.</td><td></td></tr>
<tr><td colspan="4"><b>Test 25 AC-19 (1) Access Control For Mobile Devices: The organization restricts the use of writable, removable media in organizational information systems. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>42</td><td>Review remote access control for mobile devices policy and procedures.</td><td>No mobile devices allowed.</td><td></td></tr>
<tr><td colspan="4"><b>Test 26 AC-20 (1) Use Of External Information Systems: The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization: (a) Can verify the implementation of required security controls on the external system as specified in the organization’s information security policy and security plan; or (b) Has approved information system connection or processing agreements with the organizational entity hosting the external information system. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>43</td><td>Review use of external IS policy and procedures.</td><td>No external IS allowed.</td><td></td></tr>
<tr><td colspan="4"><b>Test 27 AC-21 (1) User-Based Collaboration And Information Sharing: The information system employs automated mechanisms to enable authorized users to make information-sharing decisions based on access authorizations of sharing partners and access restrictions on information to be shared. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>44</td><td>Review user-based collaboration and information sharing</td><td>There are no automated systems for information sharing.</td><td></td></tr>
<tr><td colspan="4"><b>Test 28 AU-2 Auditable Events: The organization: a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: [Assignment: organization-defined list of auditable events; … d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: [Assignment: organization-defined subset of the auditable events defined in AU-2 to be audited along with the frequency of (or situation requiring) auditing for each identified event. NSS Defined Value a. (a) Successful and unsuccessful attempts to access, modify, or delete security objects, (b) Successful and unsuccessful logon attempts, (c) Privileged activities or other system level access, (d) Starting and ending time for user access to the system, (e) Concurrent logons from different workstations, (f) Successful and unsuccessful accesses to objects, (g) All program initiations, (h) All direct access to the information system. d. All organizations must define a list of audited events in the policy for their organization defined in accordance with AU-1., AF Defined Value []</b></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 45 | Use the AuditPol tool to review the current configuration.<br>Open a Command Prompt with elevated privileges ("Run as Administrator").<br>Enter "Auditpol /resourceSACL /type:File /view". ("File" in the /type parameter is case sensitive).<br><br>Alternately, file auditing may be configured through Windows Explorer; configured as follows<br><br>For each drive on the system, view the file auditing configuration.<br>Open Windows Explorer.<br>Right click a drive and select "Properties".<br>Select the "Security" tab.<br>Click "Advanced".<br>Select the "Auditing" tab.<br>Click "Continue" to view auditing properties.<br>Verify the following.<br><br>Type - Fail<br>Name - Everyone<br>Access - Full control<br>Apply to - This folder, subfolders and files | The following results should be displayed.<br><br>Entry:  1<br>Resource Type:  File<br>User:  Everyone<br>Flags:  Failure<br>Accesses:<br>FILE_READ_DATA<br>FILE_WRITE_DATA<br>FILE_APPEND_DATA<br>FILE_READ_EA<br>FILE_WRITE_EA<br>FILE_EXECUTE<br>FILE_DELETE_CHILD<br>FILE_READ_ATTRIBUTES<br>FILE_WRITE_ATTRIBUTES<br>DELETE<br>READ_CONTROL<br>WRITE_DAC<br>WRITE_OWNER<br><br>The command was successfully executed.<br><br>"Object Access -> File System" auditing is properly configured and drives are not formatted with NTFS<br><br>"Global Object Access Auditing" of the file system has been configured to audit all failed access attempts for the "Everyone" group | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 46 | Use the AuditPol tool to review the current configuration.<br>Open a Command Prompt with elevated privileges ("Run as Administrator").<br>Enter "Auditpol /resourceSACL /type:Key /view". ("Key" in the /type parameter is case sensitive).<br><br>Alternately, registry auditing may be configured through the registry editor.<br><br>Run "Regedit".<br>Navigate to the HKEY_LOCAL_MACHINE\SOFTWARE and HKEY_LOCAL_MACHINE\SYSTEM keys.<br>On the menu bar, select "Edit", then "Permissions".<br>Click on the "Advanced" button.<br>Select the "Auditing" tab.<br>Verify the following.<br><br>Type - Fail<br>Name - Everyone<br>Access - Full Control<br>Apply to - This key and subkeys | Entry: 1<br>Resource Type: Key<br>User: Everyone<br>Flags: Failure<br>Accesses:<br>KEY_ALL_ACCESS | |
| 47 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br><br>The policy referenced configures the following registry value:<br><br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Control\Lsa\<br><br>Value Name: SCENoApplyLegacyAuditPolicy<br><br>Value Type: REG_DWORD<br>Value: 1 | the value for “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” is set to “Enabled” | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 48 | Security Option “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” must be set to “Enabled” for the detailed auditing subcategories to be effective.<br>Use the AuditPol tool to review the current Audit Policy configuration:<br>-Open a Command Prompt with elevated privileges (“Run as Administrator”).<br>-Enter “AuditPol /get /category:*”. | Compare the Auditpol settings with the following.<br>Account Logon -> Credential Validation  - Success<br>Account Logon -> Credential Validation  - Failure<br>Account Management -> Computer Account Management  - Success<br>Account Management -> Other Account Management Events  - Success<br>Account Management -> Computer Account Management  - Failure<br>Account Management -> Other Account Management Events  - Failure<br>Detailed Tracking -> Process Creation  - Success<br>Logon/Logoff -> Special Logon  - Success<br>Object Access -> File System  - Failure<br>Object Access -> Handle Manipulation – Failure<br>Object Access -> Registry  - Failure<br>Policy Change -> Audit Policy Change  - Success<br>Policy Change -> Authentication Policy Change  - Success<br>Policy Change -> Audit Policy Change  - Failure | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| | | Privilege Use -> Sensitive Privilege Use  - Success<br>Privilege Use -> Sensitive Privilege Use  - Failure<br>System -> IPSec Driver  - Success<br>System -> Security State Change  - Success<br>System -> Security System Extension - Success<br>System -> System Integrity  - Success<br>System -> IPSec Driver  - Failure<br>System -> Security State Change  - Failure<br>System -> Security System Extension - Failure<br>System -> System Integrity  - Failure | |
| **Test 29 AU-2 (4) Auditable Events: The organization includes execution of privileged functions in the list of events to be audited by the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 49 | Review auditable events policies and procedures | include execution of privileged functions in the list of events to be audited by the information system | |
| **Test 30 AU-3 Content Of Audit Records: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event. NSS Defined Value [], AF Defined Value []** | | | |
| 50 | Reference AU-2 | Reference AU-2 | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 31 AU-3 (1) Content Of Audit Records: The information system includes [Assignment: organization-defined additional, more detailed information] in the audit records for audit events identified by type, location, or subject. NSS Defined Value [], AF Defined Value . . . at a minimum, userid, time, date, type of event/action, terminal or workstation ID, remote access, success or failure of the event/action, entity that initiated the event/action, and entity that completed the event/action . . .** | | | |
| 51 | Review the content of the audit records | . . . at a minimum, userid, time, date, type of event/action, terminal or workstation ID, remote access, success or failure of the event/action, entity that initiated the event/action, and entity that completed the event/action . . . | |
| **Test 32 AU-3 (2) Content Of Audit Records: The organization centrally manages the content of audit records generated by [Assignment: organization-defined information system components]. NSS Defined Value [], AF Defined Value . . . all information systems to the maximum extent possible.** | | | |
| 52 | Reference AU-2 | Reference AU-2 | |
| **Test 33 AU-4 Audit Storage Capacity: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. NSS Defined Value [], AF Defined Value []** | | | |
| 53 | Review audit storage capacity policy and procedures. | Storage capacity is allocated | |
| 54 | If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.<br>the following registry value exists and is configured as specified | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\Application\<br>Value Name: MaxSize<br>Type: REG_DWORD<br>Value: 0x00008000 (32768) (or greater) | |
| 55 | If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.<br>the following registry value exists and is configured as specified | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\Security\<br>Value Name: MaxSize<br>Type: REG_DWORD<br>Value: 0x00014000 (81920) (or greater) | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>56</td><td>If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.<br>the following registry value exists and is configured as specified</td><td>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup\<br>Value Name: MaxSize<br>Type: REG_DWORD<br>Value: 0x00008000 (32768) (or greater)</td><td></td></tr>
<tr><td>57</td><td>If the system is configured to send audit records directly to an audit server, this is NA. This must be documented with the ISSO.<br>the following registry value exists and is configured as specified</td><td>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\EventLog\System\<br>Value Name: MaxSize<br>Type: REG_DWORD<br>Value: 0x00008000 (32768) (or greater)</td><td></td></tr>
<tr><td colspan="4"><b>Test 34 AU-5 Response To Audit Processing Failures: The information system: a. Alerts designated organizational officials in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]. NSS Defined Value [], AF Defined Value b. shut down information system unless an alternative audit capability exists</b></td></tr>
<tr><td>58</td><td>If the system is configured to send audit records directly to an audit server, or automatically archive full logs, this is NA. This must be documented with the ISSO.<br>Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.</td><td>the value for "MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning" is set to "90%" or less<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SYSTEM\CurrentControlSet\Services\Eventlog\Security\<br>Value Name: WarningLevel<br>Value Type: REG_DWORD<br>Value: 0x0000005a (90) (or less)</td><td></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 35 AU-5 (1) Response To Audit Processing Failures: The information system provides a warning when allocated audit record storage volume reaches [Assignment: organization-defined percentage] of maximum audit record storage capacity. NSS Defined Value . . . a maximum of 75 percent, AF Defined Value []** | | | |
| 59 | Reference AU-5 | Reference AU-5 | |
| **Test 36 AU-7 Audit Reduction And Report Generation: The information system provides an audit reduction and report generation capability. NSS Defined Value [], AF Defined Value []** | | | |
| 60 | Review audit reduction and report generation | provide an audit reduction and report generation capability | |
| **Test 37 AU-7 (1) Audit Reduction And Report Generation: The information system provides the capability to automatically process audit records for events of interest based on selectable event criteria. NSS Defined Value [], AF Defined Value []** | | | |
| 61 | Review audit reduction and report generation | provide the capability to automatically process audit records for events of interest based on selectable event criteria | |
| **Test 38 AU-8 Time Stamps: The information system uses internal system clocks to generate time stamps for audit records. NSS Defined Value [], AF Defined Value []** | | | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>62</td><td>Review the following registry values:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \Software\Policies\Microsoft\W32time\Parameters\<br>Value Name: Type<br>Type: REG_SZ<br>Value: Possible values are NoSync, NTP, NT5DS, AllSync<br>And<br>Value Name: NTPServer<br>Type: REG_SZ<br>Value: "address of the time server"</td><td>Time is set to GMT<br>NOT the following;<br>"Type" has a value of "NTP" or "Allsync" AND the "NTPServer" value is set to "time.windows.com" or other unauthorized server.<br>The following is valid:<br>The referenced registry values do not exist.<br>"Type" has a value of "NoSync" or "NT5DS".<br>"Type" has a value of "NTP" or "Allsync" AND the "NTPServer" is blank or configured to an authorized time server.<br>For DoD organizations, the US Naval Observatory operates stratum 1 time servers, identified at http://tycho.usno.navy.mil/ntp.html. Time synchronization will occur through a hierarchy of time servers down to the local level. Clients and lower level servers will synchronize with an authorized time server in the hierarchy.<br>Domain joined systems are automatically configured to synchronize with domain controllers and would not be a finding unless this is changed.</td><td></td></tr>
<tr><td colspan="4"><b>Test 39 AU-8 (1) Time Stamps: The information system synchronizes internal information system clocks [Assignment: organization-defined frequency] with [Assignment: organization-defined authoritative time source]. NSS Defined Value . . . at least every 24 hours, AF Defined Value . . . an organization defined authoritative time source that complies with the provisions of ICS 500-6.</b></td></tr>
<tr><td>63</td><td>Reference AU-8</td><td>Reference AU-8</td><td></td></tr>
<tr><td colspan="4"><b>Test 40 AU-9 Protection Of Audit Information: The information system protects audit information and audit tools from unauthorized access, modification, and deletion. NSS Defined Value [], AF Defined Value []</b></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 64 | Verify the permissions on the event logs.  Standard user accounts or groups must not have access.  The default permissions listed below satisfy this requirement.<br>Navigate to the log file location. The default location is the "%SystemRoot%\System32\winevt\Logs" directory.<br>For each log file below, right click the file and select "Properties".<br>Select the "Security" tab.<br>Select the "Advanced" button, then "Continue", and respond to any UAC prompts.<br>Log Files:<br>Application.evtx<br>Security.evtx<br>System.evtx<br>Permissions:<br>Eventlog - Full Control<br>SYSTEM - Full Control<br>Administrators - Full Control | the permissions for the file are as restrictive as those listed<br>the organization may have an "Auditors" group from previous requirements, the assignment of Full Control permissions is assigned to this group | |
| 65 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> User Rights Assignment. | No accounts or groups other than the following are granted the "Manage auditing and security log" right<br>Administrators<br>the organization may have an "Auditors" group from previous requirements, the assignment of this group is to the user right | |
| **Test 41 AU-9 (2) Protection Of Audit Information: The information system backs up audit records [Assignment: organization-defined frequency] onto a different system or media than the system being audited. NSS Defined Value . . . not less than weekly, AF Defined Value []** | | | |
| 66 | Review audit storage capacity policy and procedures. | . . . not less than weekly | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td colspan="4"><b>Test 42 AU-10 Non-Repudiation: The information system protects against an individual falsely denying having performed a particular action. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>67</td><td>Review non-repudiation policies and procedures</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Test 43 AU-10 (5) Non-Repudiation: The organization employs [Selection: FIPS-validated; NSA-approved] cryptography to implement digital signatures. NSS Defined Value [], AF Defined Value … FIPS-validated or NSA-approved (as appropriate for the classification of the information system) . . . IAW 5 USC 552a (i)(3), OMB M 04-04, and A-130 Appendix 2.</b></td></tr>
<tr><td>68</td><td>Review non-repudiation policies and procedures</td><td>. . . FIPS-validated or NSA-approved (as appropriate for the classification of the information system) . . . IAW 5 USC 552a (i)(3), OMB M 04-04, and A-130 Appendix 2.</td><td></td></tr>
<tr><td colspan="4"><b>Test 44 AU-12 Audit Generation: The information system: a. Provides audit record generation capability for the list of auditable events defined in AU-2 at [Assignment: organization-defined information system components]; b. Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and c. Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. NSS Defined Value a. . . all information system and network components, AF Defined Value []</b></td></tr>
<tr><td>69</td><td>Reference AU-2</td><td>Reference AU-2</td><td></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 70 | Use the AuditPol tool to review the current configuration.<br>Open a Command Prompt with elevated privileges ("Run as Administrator").<br>Enter "Auditpol /resourceSACL /type:File /view". ("File" in the /type parameter is case sensitive).<br>Alternately, file auditing may be configured through Windows Explorer; configured as follows<br>For each drive on the system, view the file auditing configuration.<br>Open Windows Explorer.<br>Right click a drive and select "Properties".<br>Select the "Security" tab.<br>Click "Advanced".<br>Select the "Auditing" tab.<br>Click "Continue" to view auditing properties.<br>Verify the following.<br>Type - Fail<br>Name - Everyone<br>Access - Full control<br>Apply to - This folder, subfolders and files | The following results should be displayed.<br>Entry: 1<br>Resource Type: File<br>User: Everyone<br>Flags: Failure<br>Accesses:<br>FILE_READ_DATA<br>FILE_WRITE_DATA<br>FILE_APPEND_DATA<br>FILE_READ_EA<br>FILE_WRITE_EA<br>FILE_EXECUTE<br>FILE_DELETE_CHILD<br>FILE_READ_ATTRIBUTES<br>FILE_WRITE_ATTRIBUTES<br>DELETE<br>READ_CONTROL<br>WRITE_DAC<br>WRITE_OWNER<br>The command was successfully executed.<br>"Object Access -> File System" auditing is properly configured and drives are not formatted with NTFS<br>"Global Object Access Auditing" of the file system has been configured to audit all failed access attempts for the "Everyone" group | |
| **Test 45 CA-1 Security Assessment And Authorization Policies And Procedures: The organization develops, disseminates, and reviews/updates [Assignment: organization-defined frequency]: a. Formal, documented security assessment and authorization policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b. Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls. NSS Defined Value . . . at least annually if not otherwise defined in formal organizational policy, AF Defined Value []** | | | |
| 71 | Review Security Assessment And Authorization Policies And Procedures | . . . at least annually if not otherwise defined in formal organizational policy | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 46 CA-2 Security Assessments: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and - Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. NSS Defined Value b. . . at least annually, AF Defined Value []** | | | |
| 72 | Review Security Assessment And Authorization Policies And Procedures | . . . at least annually | |
| **Test 47 CA-2 (1) Security Assessments: The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 73 | Review Security Assessment And Authorization Policies And Procedures | The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system | |
| **Test 48 CA-6 Security Authorization: The organization: a. Assigns a senior-level executive or manager to the role of authorizing official for the information system; b. Ensures that the authorizing official authorizes the information system for processing before commencing operations; and c. Updates the security authorization [Assignment: organization-defined frequency] or when there is a significant change to the system. NSS Defined Value c. . . at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates., AF Defined Value []** | | | |
| 74 | Review Security Assessment And Authorization Policies And Procedures | . . . at least every three (3) years, when significant security breaches occur, whenever there is a significant change to the system, or to the environment in which the system operates. | |
| **Test 49 CA-7 (1) Continuous Monitoring: The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis. NSS Defined Value [], AF Defined Value []** | | | |
| 75 | Review continuous monitoring policies and procedures | The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 50 CM-2 (5) Baseline Configuration: The organization: (a) Develops and maintains [Assignment: organization-defined list of software programs authorized to execute on the information system]; and (b) Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system. NSS Defined Value [], AF Defined Value (a) . . . a list of software authorized to execute on the information system which includes only that software evaluated and approved by the ISSO/ISSM with the local CCB;** | | | |
| 76 | Review baseline configuration policies and procedures | . . . a list of software authorized to execute on the information system which includes only that software evaluated and approved by the ISSO/ISSM with the local CCB | |
| **Test 51 CM-6 Configuration Settings: The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. NSS Defined Value [], AF Defined Value a. . . the latest STIGS, SNAC, USGCB guidance and AF ISR configuration guides . . .** | | | |
| 77 | Verify the following:<br>The necessary documentation that identifies members of the Administrators group exists with the ISSO.<br>Each user with administrative privileges has been assigned a unique administrator account, separate from the built-in "Administrator" account.<br>Each user with administrative privileges has a separate account for performing normal (non-administrative) functions.<br>Administrators must be properly trained before being permitted to perform administrator duties.<br>Use of the built-in Administrator account must not be allowed. | the conditions are met | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 78 | Run "winver.exe". | the "About Windows" dialog box displays the following version or greater<br>"Microsoft Windows<br>Version 6.1 (Build 7601: Service Pack 1)" | |
| 79 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options. | the value for “Network access: Do not allow anonymous enumeration of SAM accounts” is set to “Enabled” | |
| 80 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options. | the value for "Network security: LAN Manager authentication level" is set to "Send NTLMv2 response only\refuse LM & NTLM" (Level 5)<br>The policy referenced configures the following registry value:<br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SYSTEM\CurrentControlSet\Control\Lsa\<br>Value Name:  LmCompatibilityLevel<br>Value Type:  REG_DWORD<br>Value:  5 | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 81 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options. | the value for “Recovery Console: Allow automatic administrative logon” is set to “Disabled”<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \Software\Microsoft\Windows NT\CurrentVersion\Setup\RecoveryConsole\<br>Value Name: SecurityLevel<br>Value Type: REG_DWORD<br>Value: 0 | |
| 82 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options. | the value for "Network access: Allow anonymous SID/Name translation" is set to "Disabled" | |
| 83 | Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options. | the value for “Accounts: Limit local account use of blank passwords to console logon only” is set to ” Enabled”<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Control\Lsa<br>Value Name: LimitBlankPasswordUse<br>Value Type: REG_DWORD<br>Value: 1 | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 84 | Verify a supported DoD antivirus product has been installed on the system.<br>The version numbers and the date of the signature can generally be checked by starting the antivirus program. The information may appear in the antivirus window or be available in the Help >> About window. The location varies from product to product. | McAfee VirusScan Enterprise 8.8 or later is installed on the system<br>the antivirus program signature has been updated within the past 7 days | |
| 85 | Determine if site policy prohibits the use of applications that access the internet, such as web browsers, or with potential internet sources, such as email, by administrative user accounts, except as necessary for local service administration. | It does | |
| 86 | Verify whether the system BIOS or controller allows removable media for the boot loader. | It does not | |
| 87 | Verify EMET v5.x or later is installed on the system. | EMET is installed and at the minimum required version | |
| 88 | Review configuration settings policies and procedures | . . . the latest STIGS, SNAC, USGCB guidance and AF ISR configuration guides . . . | |
| **Test 52 CM-7 (3) Least Functionality: The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services]. NSS Defined Value [], AF Defined Value . . . networking protocols IAW IC and DoD Ports, Protocols and Services guidance** | | | |
| 89 | Review least functionality policies and procedures | . . . networking protocols IAW IC and DoD Ports, Protocols and Services guidance | |
| 90 | Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\<br>Value Name: NoDriveTypeAutorun<br>Type: REG_DWORD<br>Value: 0x000000ff (255) | the following registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 91 | To verify whether IIS is installed, perform the following:<br>Open Control Panel.<br>Select "Programs and Features".<br>Select "Turn Windows features on or off". | the entry for "Internet Information Services" is not selected | |
| 92 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\<br>Value Name:  NoAutorun<br>Type:  REG_DWORD<br>Value:  1 | the following registry value exists and is configured as specified | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>93</td><td>Verify the operating system employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs.<br>If AppLocker is used, perform the following to view the configuration of AppLocker:<br>Open PowerShell.<br>If the AppLocker PowerShell module has not been previously imported, execute the following first:<br>Import-Module AppLocker<br>Execute the following command, substituting [c:\temp\file.xml] with a location and file name appropriate for the system:<br>Get-AppLockerPolicy -Effective | Set-Content ('c:\temp\file.xml')<br>Implementation guidance for AppLocker is available in the NSA paper "Application Whitelisting using Microsoft AppLocker" under the Microsoft Windows section of the following link:<br>https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml</td><td>an application whitelisting program is in use on the system</td><td></td></tr>
<tr><td colspan="4"><b>Test 53 CM-8 (3) Information System Component Inventory: The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the addition of unauthorized components/devices into the information system; and (b) Disables network access by such components/devices or notifies designated organizational officials. NSS Defined Value [], AF Defined Value (a) . . . continuously</b></td></tr>
<tr><td>94</td><td>Review Information System Component Inventory policies and procedures</td><td>. . . continuously</td><td></td></tr>
<tr><td colspan="4"><b>Test 54 CP-10 (2) Information System Recovery And Reconstitution: The information system implements transaction recovery for systems that are transaction-based. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>95</td><td>Not applicable</td><td>NA</td><td></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 55 IA-2 Identification And Authentication (Organizational Users): The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users). NSS Defined Value [], AF Defined Value []** | | | |
| 96 | Determine if any shared accounts exist. If no shared accounts exist, this is NA.<br>Any shared account must be documented with the ISSO. Documentation must include the reason for the account, who has access to this account, and how the risk of using a shared account (which provides no individual identification and accountability) is mitigated. | documentation exists and is current<br>Note: As an example, a shared account may be permitted for a help desk or a site security personnel machine, if that machine is standalone and has no access to the network. | |
| 97 | Using the DUMPSEC utility:<br>Select “Dump Users as Table” from the “Report” menu.<br>Select the available fields in the following sequence, and click on the “Add” button for each entry:<br>UserName<br>SID<br>PswdRequired<br>PswdExpires<br>LastLogonTime<br>AcctDisabled<br>Groups | No accounts listed in the user report have a “No” in the “PswdRequired” column<br>Note: Some built-in or application-generated accounts (e.g., Guest, IWAM_, IUSR, etc.) will not have this flag set, even though there are passwords present. It can be set by entering the following on a command line: “Net user <account_name> /passwordreq:yes”. | |
| 98 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options. | the value for "Accounts: Administrator account status" is set to "Disabled" | |
| **Test 56 IA-2 (1) Identification And Authentication (Organizational Users): The information system uses multifactor authentication for network access to privileged accounts. NSS Defined Value [], AF Defined Value []** | | | |
| 99 | Review identification and authentication for organizational users policies and procedures | . . . uses multifactor authentication for network access to privileged accounts | |
| **Test 57 IA-2 (2) Identification And Authentication (Organizational Users): The information system uses multifactor authentication for network access to non-privileged accounts. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 100 | Review identification and authentication for organizational users policies and procedures | . . . uses multifactor authentication for network access to non-privileged accounts |  |
| **Test 58 IA-2 (3) Identification And Authentication (Organizational Users): The information system uses multifactor authentication for local access to privileged accounts. NSS Defined Value [], AF Defined Value []** |  |  |  |
| 101 | Review identification and authentication for organizational users policies and procedures | . . . uses multifactor authentication for local access to privileged accounts |  |
| **Test 59 IA-2 (4) Identification And Authentication (Organizational Users): The information system uses multifactor authentication for local access to non-privileged accounts. NSS Defined Value [], AF Defined Value []** |  |  |  |
| 102 | Consult documentation to determine if the system is capable of CAC, PIV compliant hardware token, or Alternate Logon Token (ALT) for authentication. | Interview the system administrator (SA) to determine if all accounts not exempted by policy are using multi factor authentication. Non-exempt accounts are using multi factor authentication. |  |
| **Test 60 IA-2 (8) Identification And Authentication (Organizational Users): The information system uses [Assignment: organization-defined replay resistant authentication mechanisms] for network access to privileged accounts. NSS Defined Value [], AF Defined Value . . . SSH/TLS based access or equivalent** |  |  |  |
| 103 | Review identification and authentication for organizational users policies and procedures | . . . SSH/TLS based access or equivalent |  |
| **Test 61 IA-2 (9) Identification And Authentication (Organizational Users): The information system uses [Assignment: organization-defined replay resistant authentication mechanisms] for network access to non-privileged accounts. NSS Defined Value [], AF Defined Value . . . SSH/TLS based access or equivalent** |  |  |  |
| 104 | Review identification and authentication for organizational users policies and procedures | . . . SSH/TLS based access or equivalent |  |
| **Test 62 IA-3 Device Identification And Authentication: The information system uniquely identifies and authenticates [Assignment: organization-defined list of specific and/or types of devices] before establishing a connection. NSS Defined Value . . . all network connected endpoint devices, AF Defined Value []** |  |  |  |
| 105 | Review device level identification and authentication policies and procedures | . . . all network connected endpoint devices |  |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 106 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SYSTEM\CurrentControlSet\Control\LSA\<br>Value Name: UseMachineId<br>Type: REG_DWORD<br>Value: 1 | the value for "Network Security: Allow Local System to use computer identity for NTLM" is set to "Enabled" | |
| **Test 63 IA-3 (1) Device Identification And Authentication: The information system authenticates devices before establishing remote and wireless network connections using bidirectional authentication between devices that is cryptographically based. NSS Defined Value [], AF Defined Value []** | | | |
| 107 | Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \Software\Policies\Microsoft\Windows NT\Rpc\<br>Value Name: RestrictRemoteClients<br>Type: REG_DWORD<br>Value: 1 | the following registry value exists and is configured as specified | |
| 108 | Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \Software\Policies\Microsoft\Windows NT\Rpc\<br>Value Name: EnableAuthEpResolution<br>Type: REG_DWORD<br>Value: 1 | the following registry value exists and is configured as specified | |
| **Test 64 IA-3 (2) Device Identification And Authentication: The information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based. NSS Defined Value [], AF Defined Value []** | | | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>109</td><td>Review device level identification and authentication policies and procedures</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Test 65 IA-3 (3) Device Identification And Authentication: The organization standardizes, with regard to dynamic address allocation, Dynamic Host Control Protocol (DHCP) lease information and the time assigned to devices, and audits lease information when assigned to a device. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>110</td><td>Review device level identification and authentication policies and procedures</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Test 66 IA-4 (4) Identifier Management: The organization manages user identifiers by uniquely identifying the user as [Assignment: organization-defined characteristic identifying user status]. NSS Defined Value A contractor or government employee and citizenship, AF Defined Value []</b></td></tr>
<tr><td>111</td><td>Review identifier management policies and procedures</td><td>A contractor or government employee and citizenship</td><td></td></tr>
<tr><td>112</td><td>Run the DUMPSEC utility.<br>Select "Dump Users as Table" from the "Report" menu.<br>Select the following fields, and click "Add" for each entry:<br>UserName<br>SID<br>LastLogonTime<br>AcctDisabled<br>Review the "LastLogonTime".<br>The following accounts are exempt:<br>Built-in administrator account (SID ending in 500)<br>Built-in guest account (SID ending in 501)<br>Application accounts<br>Disabled accounts<br>Review the list to determine the finding validity for each account reported.<br>If the organization has a need for special purpose local user accounts such as a backup administrator account, this must be documented with the ISSO.</td><td>No enabled accounts have not been logged on to within the past 35 days</td><td></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 67 IA-5 (1) Authenticator Management: The information system, for password-based authentication: (a) Enforces minimum password complexity of [Assignment: organization-defined requirements for case sensitivity, number of characters, mix of upper case letters, lower case letters, numbers, and special characters, including minimum requirements for each type] (b) Enforces at least a [Assignment: organization-defined number of changed characters] when new passwords are created; … (d) Enforces password minimum and maximum lifetime restrictions of [Assignment: organization-defined numbers for lifetime minimum, lifetime maximum]; and (e) Prohibits password reuse for [Assignment: organization-defined number] generations. NSS Defined Value (a) a case sensitive, 8- character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (b) at least four (d) 24 hours minimum and 180 days maximum (e) a minimum of 10 NOTE: The above requirements do not apply to one-time use passwords., AF Defined Value []** | | | |
| 113 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Account Policies -> Password Policy. | the value for “Password must meet complexity requirements” is set to "Enabled"<br>the value for "Store password using reversible encryption" is disabled | |
| 114 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Control\Lsa\<br>Value Name: NoLMHash<br>Value Type: REG_DWORD<br>Value: 1 | the value for “Network security: Do not store LAN Manager hash value on next password change” is set to “Enabled” | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 115 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Account Policies >> Password Policy. | the value for the "Maximum password age" is less than "60" days<br>the value is not set to "0" (never expires)<br>the value for the "Minimum password age" is at least "1" day<br>the value for the "Minimum password length" is more than 14 characters<br>the value for "Enforce password history" is more than "24" passwords | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 116 | The site should have a local policy to ensure that passwords for application/service accounts are at least 15 characters in length and meet complexity requirements for all passwords.  Application/service account passwords manually generated and entered by a system administrator must be changed at least annually or whenever a system administrator that has knowledge of the password leaves the organization.<br>Interview the system administrators on their policy for application/service accounts.<br>Using the DUMPSEC utility:<br>Select "Dump Users as Table" from the "Report" menu.<br>Select the available fields in the following sequence, and click on the "Add" button for each entry:<br>UserName<br>SID<br>PswdRequired<br>PswdExpires<br>PswdLastSetTime<br>LastLogonTime<br>AcctDisabled<br>Groups | meets the requirements<br>No application accounts listed in the Dumpsec user report have a date older than one year in the "PwsdLastSetTime" column | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 117 | Run the DUMPSEC utility.<br>Select "Dump Users as Table" from the "Report" menu.<br>Select the following fields, and click "Add" for each entry.<br>UserName<br>SID<br>PswdExpires<br>AcctDisabled<br>Groups<br>The following are exempt from this requirement:<br>Built-in Administrator Account<br>Application Accounts<br>Accounts that meet the requirements for allowable exceptions must be documented with the ISSO. | No accounts have "No" in the "PswdExpires" column | |
| **Test 68 IA-5 (2) Authenticator Management: The information system, for PKI-based authentication: (a) Validates certificates by constructing a certification path with status information to an accepted trust anchor; (b) Enforces authorized access to the corresponding private key; and (c) Maps the authenticated identity to the user account. NSS Defined Value [], AF Defined Value []** | | | |
| 118 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Subkey:  \Software\Policies\Microsoft\SystemCertificates\AuthRoot\<br>Value Name:  DisableRootAutoUpdate<br>Type:  REG_DWORD<br>Value:  1 | the registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 119 | Verify the DoD Root CA 2 certificate is installed as a Trusted Root Certification Authority using the Certificates MMC snap-in:<br>Run "MMC".<br>Select "File", "Add/Remove Snap-in".<br>Select "Certificates", click "Add".<br>Select "Computer account", click "Next".<br>Select "Local computer: (the computer this console is running on)", click "Finish".<br>Click "OK".<br>Expand "Certificates" and navigate to "Trusted Root Certification Authorities\Certificates".<br>Search for "DoD Root CA 2" under "Issued To" in the center pane. | An entry for "DoD Root CA 2" | |
| | Select DoD Root CA 2.<br>Right click and select "Open".<br>Select the "Details" Tab.<br>Scroll to the bottom and select "Thumbprint Algorithm".<br>Verify the Value is "sha1". | the value for "Thumbprint Algorithm" is "sha1" | |
| | Next select "Thumbprint". | the value for the "Thumbprint" field is<br>"Need the value for the particular DoD network in question" | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 120 | Verify the ECA Root CA 2 certificate is installed systems as a Trusted Root Certification Authority using the Certificates MMC snap-in.<br>Run “MMC”<br>Select “File”, “Add/Remove Snap-in…”<br>Select “Certificates”, click “Add”<br>Select “Computer account”, click “Next”<br>Select “Local computer: (the computer this console is running on)”, click “Finish”<br>Click “OK”<br>Expand “Certificates” and navigate to “Trusted Root Certification Authorities\Certificates”<br>Search for “ECA Root CA 2” under “Issued To” in the center pane<br>Select “ECA Root CA 2”<br>Right click and select “Open”<br>Select the “Details” Tab<br>Scroll to the bottom and select “Thumbprint Algorithm”<br>Verify the Value is “sha1”,<br>Next select "Thumbprint". | An entry for “ECA Root CA 2”<br>the value for "Thumbprint Algorithm" is "sha1"<br>the value for the "Thumbprint" field is<br>"Need the value for the particular external network in question" | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 121 | Verify the DoD Root CA 2 certificate issued by DoD Interoperability Root CA 1 is installed on NIPRNet systems as an Untrusted Certificate using the Certificates MMC snap-in.<br>Run “MMC”<br>Select “File”, “Add/Remove Snap-in…”<br>Select “Certificates”, click “Add”<br>Select “Computer account”, click “Next”<br>Select “Local computer: (the computer this console is running on)”, click “Finish”<br>Click “OK”<br>Expand “Certificates” and navigate to “Untrusted Certificates\Certificates”<br>Search in the center pane for “DoD Root CA 2” under “Issued To” with “DoD Interoperability Root CA 1” as “Issued By”<br>Select “DoD Root CA 2”<br>Right click and select “Open”<br>Select the “Details” Tab<br>Scroll to the bottom and select “Thumbprint Algorithm”<br>Verify the Value is “sha1”,<br>Next select “Thumbprint” | An entry for "DoD Root CA 2"<br>the value for "Thumbprint Algorithm" is "sha1"<br>the value for the "Thumbprint" field is<br>"Need the value for the particular DoD network in question" | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 122 | Verify the DoD Root CA 2 certificate issued by US DoD CCEB Interoperability Root CA 1 is installed on NIPRNet systems as an Untrusted Certificate using the Certificates MMC snap-in:<br>Run "MMC".<br>Select "File", "Add/Remove Snap-in".<br>Select "Certificates", click "Add".<br>Select "Computer account", click "Next".<br>Select "Local computer: (the computer this console is running on)", click "Finish".<br>Click "OK".<br>Expand "Certificates" and navigate to "Untrusted Certificates\Certificates".<br>Search in the center pane for "DoD Root CA 2" under "Issued To" with "US DoD CCEB Interoperability Root CA 1" as "Issued By".<br>Select the certificate.<br>Right click and select "Open".<br>Select the "Details" Tab.<br>Scroll to the bottom and select "Thumbprint Algorithm".<br>Verify the Value is "sha1".<br>Next select “Thumbprint” | An entry for this certificate<br>the value for "Thumbprint Algorithm" is not "sha1"<br>the value for the "Thumbprint" field is<br>"Need the value for the particular DoD network in question" | |
| **Test 69 IA-5 (7) Authenticator Management: The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys. NSS Defined Value [], AF Defined Value []** | | | |
| 123 | Review the software and script approval process | The software approval process utilizes an automated mechanism that looks for likely embedded authenticators in the source code or in scripts. | |
| **Test 70 IA-6 Authenticator Feedback: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. NSS Defined Value [], AF Defined Value []** | | | |
| 124 | Log out of the system | User is logged out | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td>125</td><td>Log into the system</td><td>When entering the password into the system, there should be no feedback (i.e. no asterisks representing the number of characters entered)</td><td></td></tr>
<tr><td colspan="4"><b>Test 71 IA-7 Cryptographic Module Authentication: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>126</td><td>Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Kerberos\Parameters\<br>Value Name:  SupportedEncryptionTypes<br>Type:  REG_DWORD<br>Value:  0x7ffffffc (2147483644)</td><td>the value for "Network Security: Configure encryption types allowed for Kerberos" is set to "Enabled" with only the following selected<br>RC4_HMAC_MD5<br>AES128_HMAC_SHA1<br>AES256_HMAC_SHA1<br>DES_CBC_CRC and DES_CBC_MD5 should not be selected</td><td></td></tr>
<tr><td colspan="4"><b>Test 72 PL-2 System Security Plan: The organization: a. Develops a security plan for the information system that: - Is consistent with the organization’s enterprise architecture; - Explicitly defines the authorization boundary for the system; - Describes the operational context of the information system in terms of missions and business processes; - Provides the security categorization of the information system including supporting rationale; - Describes the operational environment for the information system; - Describes relationships with or connections to other information systems; - Provides an overview of the security requirements for the system; - Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and - Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Reviews the security plan for the information system [Assignment: organization-defined frequency]; and c. Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments. NSS Defined Value b. . . at least annually or when required due to system modifications, AF Defined Value []</b></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 127 | Review the System Security Plan | A System Security Plan exists and it:<br>- Is consistent with the organization’s enterprise architecture;<br>- Explicitly defines the authorization boundary for the system;<br>- Describes the operational context of the information system in terms of missions and business processes;<br>- Provides the security categorization of the information system including supporting rationale;<br>- Describes the operational environment for the information system;<br>- Describes relationships with or connections to other information systems;<br>- Provides an overview of the security requirements for the system;<br>- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and<br>- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; | |
| **Test 73 PL-2 (1) System Security Plan: The organization: (a) Develops a security Concept of Operations (CONOPS) for the information system containing, at a minimum: (i) the purpose of the system; (ii) a description of the system architecture; (iii) the security authorization schedule; and (iv) the security categorization and associated factors considered in determining the categorization; and (b) Reviews and updates the CONOPS [Assignment: organization-defined frequency]. NSS Defined Value (b) . . . annually or as required due to system modifications, AF Defined Value []** | | | |
| 128 | Review System Security Plan policies and procedures | . . . annually or as required due to system modifications | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 74 PL-2 (2) System Security Plan: The organization develops a functional architecture for the information system that identifies and maintains: (a) External interfaces, the information being exchanged across the interfaces, and the protection mechanisms associated with each interface; (b) User roles and the access privileges assigned to each role; (c) Unique security requirements; (d) Types of information processed, stored, or transmitted by the information system and any specific protection needs in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; and (e) Restoration priority of information or information system services. NSS Defined Value [], AF Defined Value []** | | | |
| 129 | Review System Security Plan policies and procedures | Functional architecture | |
| **Test 75 RA-2 Security Categorization: The organization: a. Categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Documents the security categorization results (including supporting rationale) in the security plan for the information system; and c. Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. NSS Defined Value [], AF Defined Value []** | | | |
| 130 | Complete the Discovery Meeting Checklist | The outcomes of the discovery meeting are;<br>- System security categorization, Reference FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, p. 1<br>- The information owner/information system owner identifies the types of information associated with the information system and assigns a security impact value (low, moderate, high) for the security objectives of confidentiality, integrity, or availability to each information type. | |
| **Test 76 SA-2 Allocation Of Resources: The organization: a. Includes a determination of information security requirements for the information system in mission/business process planning; b. Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and c. Establishes a discrete line item for information security in organizational programming and budgeting documentation. NSS Defined Value [], AF Defined Value []** | | | |
| 131 | Review allocation of resources | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 77 SA-3 Life Cycle Support: The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities. NSS Defined Value [], AF Defined Value []** | | | |
| 132 | Review life cycle support | | |
| **Test 78 SA-4 Acquisitions: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards: a. Security functional requirements/specifications; b. Security-related documentation requirements; and c. Developmental and evaluation-related assurance requirements. NSS Defined Value [], AF Defined Value []** | | | |
| 133 | Review acquisitions policies and procedures | Included, but not limited to, in the list of artifacts are;<br>- Security Plan (SP) or System Security Authorization Agreement (SSAA) with Attachment 11s<br>- Trusted Facility Manuals (TFM)<br>- Software Version Description Documents (SVDD)<br>- Security Features Users Guides (SFUG)<br>- Initial Equipment Inventory with Hostnames and IP Addresses included<br>- Diagrams/Drawings<br>- Site Preparation Requirements and Installation Plans (SPRIP) | |
| **Test 79 SA-4 (6) Acquisitions: The organization: (a) Employs only government off-the-shelf (GOTS) or commercial off-the-shelf (COTS) information assurance (IA) and IA-enabled information technology products that composes an NSA-approved solution to protect classified information when the networks used to transmit the information are at a lower classification level than the information being transmitted; and (b) Ensures that these products have been evaluated and/or validated by the NSA or in accordance with NSA-approved procedures. NSS Defined Value [], AF Defined Value []** | | | |
| 134 | Review acquisitions policies and procedures | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 80 SA-5 Information System Documentation: The organization: a. Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes: - Secure configuration, installation, and operation of the information system; - Effective use and maintenance of security features/functions; and - Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and b. Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes: - User-accessible security features/functions and how to effectively use those security features/functions; - Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and - User responsibilities in maintaining the security of the information and information system; and c. Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent. NSS Defined Value [], AF Defined Value []** | | | |
| 135 | Review information system documentation | | |
| **Test 81 SA-5 (1) Information System Documentation: The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing. NSS Defined Value [], AF Defined Value []** | | | |
| 136 | Review information system documentation | | |
| **Test 82 SA-5 (2) Information System Documentation: The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing. NSS Defined Value [], AF Defined Value []** | | | |
| 137 | Review information system documentation | | |
| **Test 83 SA-6 Software Usage Restrictions: The organization: a. Uses software and associated documentation in accordance with contract agreements and copyright laws; b. Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and c. Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. NSS Defined Value [], AF Defined Value []** | | | |
| 138 | Review software usage restrictions | | |
| **Test 84 SA-8 Security Engineering Principles: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 139 | Review security engineering principles | | |

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td colspan="4"><b>Test 85 SA-9 External Information System Services: The organization: a. Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Monitors security control compliance by external service providers. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>140</td><td>Review external information system services</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Test 86 SA-9 (1) External Information System Services: The organization: (a) Conducts an organizational assessment of risk prior to the acquisition or outsourcing of dedicated information security services; and b. Ensures that the acquisition or outsourcing of dedicated information security services is approved by [Assignment: organization-defined senior organizational official]. NSS Defined Value b. Chief Information Officer, AF Defined Value []</b></td></tr>
<tr><td>141</td><td>Review external information system services</td><td>Chief Information Officer</td><td></td></tr>
<tr><td colspan="4"><b>Test 87 SA-10 Developer Configuration Management: The organization requires that information system developers/integrators: a. Perform configuration management during information system design, development, implementation, and operation; b. Manage and control changes to the information system; c. Implement only organization-approved changes; d. Document approved changes to the information system; and e. Track security flaws and flaw resolution. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>142</td><td>Review developer configuration management</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Test 88 SA-10 (1) Developer Configuration Management: The organization requires that information system developers/integrators provide an integrity check of software to facilitate organizational verification of software integrity after delivery. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>143</td><td>Review developer configuration management</td><td></td><td></td></tr>
<tr><td colspan="4"><b>Test 89 SA-11 Developer Security Testing: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers): a. Create and implement a security test and evaluation plan; b. Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and c. Document the results of the security testing/evaluation and flaw remediation processes. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>144</td><td>Review developer security testing</td><td>. . . the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements</td><td></td></tr>
</table>

<table>
<tr><th>Step</th><th>Step Description</th><th>Expected Results/Comments</th><th>P/F</th></tr>
<tr><td colspan="4"><b>Test 90 SA-12 Supply Chain Protection: The organization protects against supply chain threats by employing: [Assignment: organization-defined list of measures to protect against supply chain threats] as part of a comprehensive, defense-in-breadth information security strategy. NSS Defined Value Measures in accordance with CNSS Directive 505, Supply Chain Risk Management., AF Defined Value []</b></td></tr>
<tr><td>145</td><td>Review supply chain protection</td><td>Measures in accordance with CNSS Directive 505, Supply Chain Risk Management.</td><td></td></tr>
<tr><td colspan="4"><b>Test 91 SA-12 (2) Supply Chain Protection: The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>146</td><td>Review supply chain protection</td><td>Supplier review may include analysis of supplier processes used to design, develop, test, implement, verify, deliver, and support information systems, system components, and information system services; and assessment of supplier training and experience in developing systems, components, or services with the required security capability.</td><td></td></tr>
<tr><td colspan="4"><b>Test 92 SC-2 Application Partitioning: The information system separates user functionality (including user interface services) from information system management functionality. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>147</td><td>Review application partitioning policies and procedures</td><td>user functionality is limited by group permission assignment</td><td></td></tr>
<tr><td colspan="4"><b>Test 93 SC-2 (1) Application Partitioning: The information system prevents the presentation of information system management-related functionality at an interface for general (i.e., non-privileged) users. NSS Defined Value [], AF Defined Value []</b></td></tr>
<tr><td>148</td><td>Review application partitioning policies and procedures</td><td>user must enter privileged (.priv) credentials to access management functions of the system</td><td></td></tr>
<tr><td colspan="4"><b>Test 94 SC-4 Information In Shared Resources: The information system prevents unauthorized and unintended information transfer via shared system resources. NSS Defined Value [], AF Defined Value []</b></td></tr>
</table>

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 149 | Open the Computer Management Console.<br>Expand the "System Tools" object in the left pane.<br>Expand the "Shared Folders" object.<br>Select the "Shares" object.<br>Right click any user-created shares (ignore administrative shares; the system will prompt you if Properties are selected for administrative shares).<br>Select "Properties".<br>Select the "Share Permissions" tab. | user-created file shares have been reconfigured to remove ACL permissions from the "Everyone" group<br>If shares created by applications require the "Everyone" group, this must be documented with the ISSO. | |
| 150 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SYSTEM\CurrentControlSet\Control\Lsa\<br>Value Name:   RestrictAnonymous<br>Value Type:   REG_DWORD<br>Value:   1 | the value for "Network access: Do not allow anonymous enumeration of SAM accounts and shares" is set to "Enabled" | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 151 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\<br>Value Name: NullSessionPipes<br>Value Type: REG_MULTI_SZ<br>Value: (blank) | the value for "Network access: Named pipes that can be accessed anonymously" contains NO entries<br>Note: Legitimate applications may add entries to this registry value. If an application requires these entries to function properly, it should be documented with the ISSO. Documentation should contain supporting information from the vendor's instructions. | |
| 152 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedExactPaths\<br>Value Name: Machine<br>Value Type: REG_MULTI_SZ<br>Value: As defined in expected results | the value for "Network access: Remotely accessible registry paths" contains the following entries ONLY<br>System\CurrentControlSet\Control\ProductOptions<br>System\CurrentControlSet\Control\Server Applications<br>Software\Microsoft\Windows NT\CurrentVersion | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 153 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\LanManServer\Parameters\<br>Value Name:  NullSessionShares<br>Value Type:  REG_MULTI_SZ<br>Value:  (Blank) | the value for “Network access: Shares that can be accessed anonymously” includes NO entries | |
| 154 | Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\<br>Value Name: fAllowToGetHelp<br>Type: REG_DWORD<br>Value: 0 | the following registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 155 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Control\Lsa\<br>Value Name:  ForceGuest<br>Value Type:  REG_DWORD<br>Value:  0 | the value for “Network access: Sharing and security model for local accounts” is set to “Classic - local users authenticate as themselves” | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 156 | -Users must be trained to include the following:<br>-Users must know who they can accept a remote assistance offer from. The remote assistance offer must be in response to a help desk request or confirmed with the help desk if an unsolicited remote assistance offer comes through.<br>-Users must know how to accept a request, allow view or control, and disconnect a remote assistance session.<br>-Users must monitor the remote assistance activity at the workstation while it is occurring.<br>-The support personnel allowed to offer remote assistance (helpers) must be limited and documented.<br>-Port 3389 must be blocked at the perimeter to prevent other access.<br>Accounts and groups authorized to offer remote assistance (helpers) are identified in the following registry key.<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\ Microsoft\Windows NT\Terminal Services\ RAUnsolicit\ | Each account or group will be listed under a separate value name with the value equaling the value name as in the following examples:<br>Value Name: Administrators<br>Value Type: REG_SZ<br>Value: Administrators<br>Value Name: TestUser<br>Value Type: REG_SZ<br>Value: TestUser | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 157 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br><br>The policy referenced configures the following registry value:<br><br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\AllowedPaths\<br><br>Value Name:  Machine<br><br>Value Type:  REG_MULTI_SZ<br>Value:  As defined in policy above | the value for "Network access: Remotely accessible registry paths and sub-paths" contains ONLY entries following<br><br>Software\Microsoft\OLAP Server<br>Software\Microsoft\Windows NT\CurrentVersion\Perflib<br>Software\Microsoft\Windows NT\CurrentVersion\Print<br>Software\Microsoft\Windows NT\CurrentVersion\Windows<br>System\CurrentControlSet\Control\ContentIndex<br>System\CurrentControlSet\Control\Print\Printers<br>System\CurrentControlSet\Control\Terminal Server<br>System\CurrentControlSet\Control\Terminal Server\UserConfig<br>System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration<br>System\CurrentControlSet\Services\Eventlog<br>System\CurrentControlSet\Services\Sysmonlog<br><br>Note:  Legitimate applications may add entries to this registry value. If an application requires these entries to function properly, it is documented with the ISSO. Documentation should contain supporting information from the vendor's instructions. | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 158 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\LanManServer\Parameters\<br>Value Name: RestrictNullSessAccess<br>Value Type: REG_DWORD<br>Value: 1 | the value for “Network access: Restrict anonymous access to Named Pipes and Shares” is set to “Enabled” | |
| 159 | Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \Software\Policies\Microsoft\Windows NT\Terminal Services\<br>Value Name: fDisableCdm<br>Type: REG_DWORD<br>Value: 1 | the registry value exists and is configured as specified | |
| **Test 95 SC-5 Denial Of Service Protection: The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined list of types of denial of service attacks or reference to source for current list]. NSS Defined Value Consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, physical destruction or alteration of network components, AF Defined Value []** | | | |
| 160 | Review denial of service protection | Consumption of scarce, limited, or non-renewable resources, destruction or alteration of configuration information, physical destruction or alteration of network components | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 161 | Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \System\CurrentControlSet\Services\Tcpip\Parameters\<br>Value Name: KeepAliveTime<br>Value Type:  REG_DWORD<br>Value:  300000 | the value for “MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds” is set to “300000 or 5 minutes (recommended)” or more | |
| 162 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SYSTEM\CurrentControlSet\Services\Netbt\Parameters\<br>Value Name:  NoNameReleaseOnDemand<br>Value Type:  REG_DWORD<br>Value:  1 | the value for "MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers" is set to "Enabled" | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 163 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br><br>Registry Hive: HKEY_LOCAL_MACHINE<br>Subkey: \System\CurrentControlSet\Services\Tcpip\Parameters\<br><br>Value Name: PerformRouterDiscovery<br><br>Value Type:  REG_DWORD<br>Value:  0 | he value for “MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)” is set to “Disabled” | |
| 164 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br><br>The policy referenced configures the following registry value:<br><br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\<br><br>Value Name:  TcpMaxDataRetransmissions<br><br>Value Type:  REG_DWORD<br>Value:  3 (or less) | the value for "MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)" is set to "3" or more | |
| 165 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Subkey:  \Software\Policies\Microsoft\Windows\Explorer\<br><br>Value Name: NoHeapTerminationOnCorruption<br><br>Type:  REG_DWORD<br>Value:  0 | the following registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 96 SC-5 (1) Denial Of Service Protection: The information system restricts the ability of users to launch denial of service attacks against other information systems or networks. NSS Defined Value [], AF Defined Value []** | | | |
| 166 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Control\Lsa<br>Value Name: AuditBaseObjects<br>Value Type: REG_DWORD<br>Value: 0 | the value for "Audit: Audit the access of global system objects" is set to "Disabled" | |
| 167 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Control\Lsa<br>Value Name: FullPrivilegeAuditing<br>Value Type: REG_Binary<br>Value: 0 | the value for “Audit: Audit the use of Backup and Restore privilege” is set to “Disabled” | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 97 SC-7 Boundary Protection: The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. NSS Defined Value [], AF Defined Value []** | | | |
| 168 | Review boundary protection | | |
| **Test 98 SC-7 (1) Boundary Protection: The organization physically allocates publicly accessible information system components to separate sub-networks with separate physical network interfaces. NSS Defined Value [], AF Defined Value []** | | | |
| 169 | Review boundary protection | | |
| **Test 99 SC-7 (2) Boundary Protection: The information system prevents public access into the organizations internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. NSS Defined Value [], AF Defined Value []** | | | |
| 170 | Review boundary protection | | |
| **Test 100 SC-7 (3) Boundary Protection: The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic. NSS Defined Value [], AF Defined Value []** | | | |
| 171 | Review boundary protection | | |
| **Test 101 SC-7 (4) Boundary Protection: The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface; (c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need. NSS Defined Value (e). . . at least every 6 months, AF Defined Value []** | | | |
| 172 | Review boundary protection policies and procedures | . . . at least every 6 months | |
| **Test 102 SC-7 (5) Boundary Protection: The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception). NSS Defined Value [], AF Defined Value []** | | | |
| 173 | Review boundary protection | | |
| **Test 103 SC-7 (7) Boundary Protection: The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks. NSS Defined Value [], AF Defined Value []** | | | |
| 174 | Review boundary protection | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 104 SC-7 (8) Boundary Protection: The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers within the managed interfaces of boundary protection devices. NSS Defined Value (1) . . . all internal communications traffic, except traffic specifically exempted by the Authorizing Official or organizational policy . . . (2) . . . networks outside the control of the organization, AF Defined Value []** | | | |
| 175 | Review boundary protection scheme policies and procedures | . . . all internal communications traffic, except traffic specifically exempted by the Authorizing Official or organizational policy<br>. . . networks outside the control of the organization | |
| **Test 105 SC-7 (11) Boundary Protection: The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination. NSS Defined Value [], AF Defined Value []**<br>**SC-7 (14) Boundary Protection: The organization protects against unauthorized physical connections across the boundary protections implemented at [Assignment: organization-defined list of managed interfaces]. NSS Defined Value . . . cross domain solutions and controlled interfaces., AF Defined Value []** | | | |
| 176 | Read system Interface Control Document and interview system administrators | . . . cross domain solutions and controlled interfaces | |
| 177 | Review boundary protection | Only approved incoming routes should be present | |
| **Test 106 SC-7 (12) Boundary Protection: The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices. NSS Defined Value [], AF Defined Value []** | | | |
| 178 | Review boundary protection | Local firewall is used | |
| **Test 107 SC-7 (13) Boundary Protection: The organization isolates [Assignment: organization defined key information security tools, mechanisms, and support components] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system. NSS Defined Value [], AF Defined Value . . . at a minimum, vulnerability scanning tools, audit log servers, patch servers, and Computer Network Defense (CND) tools . . .** | | | |
| 179 | Review boundary protection | | |
| **Test 109 SC-7 (18) Boundary Protection: The information system prevents discovery of specific system components (or devices) composing a managed interface. NSS Defined Value [], AF Defined Value []** | | | |
| 180 | Review boundary protection | | |
| **Test 110 SC-8 Transmission Integrity: The information system protects the integrity of transmitted information. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 181 | Review the system Interface control document (ICD) | Check for use of protocols that ensure integrity of transmissions (i.e. TCP which everyone uses) | |
| 182 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\Netlogon\Parameters\<br>Value Name: SignSecureChannel<br>Value Type: REG_DWORD<br>Value: 1 | the value for “Domain Member: Digitally sign secure channel data (when possible)” is set to “Enabled” | |
| 183 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\Netlogon\Parameters\<br>Value Name: SealSecureChannel<br>Value Type: REG_DWORD<br>Value: 1 | the value for “Domain Member: Digitally encrypt secure channel data (when possible)” is set to “Enabled”<br>Also, can be<br>the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled” | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 184 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\Netlogon\Parameters\<br>Value Name: RequireSignOrSeal<br>Value Type: REG_DWORD<br>Value: 1 | the value for “Domain Member: Digitally encrypt or sign secure channel data (always)” is set to “Enabled” | |
| 185 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\Netlogon\Parameters\<br>Value Name: RequireStrongKey<br>Value Type: REG_DWORD<br>Value: 1 | the value for “Domain Member: Require Strong (Windows 2000 or Later) Session Key” is set to “Enabled”<br>Warning: This setting may prevent a system from being joined to a domain if not configured consistently between systems. | |
| **Test 111 SC-9 Transmission Confidentiality: The information system protects the confidentiality of transmitted information. NSS Defined Value [], AF Defined Value []** | | | |
| 186 | Review the system Interface control document (ICD) | Check for use of secure protocols in the ICD. The use of unsecured protocols is a finding. | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 112 SC-9 (1) Transmission Confidentiality: The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by [Assignment: organization-defined alternative physical measures]. NSS Defined Value A protected distribution system or in a controlled access area accredited for open storage., AF Defined Value []** | | | |
| 187 | Review the system Interface control document (ICD) | Check for use of secure protocols in the ICD. The use of unsecured protocols is a finding. | |
| **Test 113 SC-9 (2) Transmission Confidentiality: The information system maintains the confidentiality of information during aggregation, packaging, and transformation in preparation for transmission. NSS Defined Value [], AF Defined Value []** | | | |
| 188 | Review the system Interface control document (ICD) | Check for use of secure protocols in the ICD. The use of unsecured protocols is a finding. | |
| **Test 114 SC-10 Network Disconnect: The information system terminates the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity. NSS Defined Value . . . not more than 1 hour, AF Defined Value []** | | | |
| 189 | Review network disconnect policies and procedures | . . . not more than 1 hour | |
| 190 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options. | the value for "Network security: Force logoff when logon hours expire" is set to "Enabled" | |
| 191 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Subkey:  \Software\Policies\Microsoft\Windows NT\Terminal Services\<br>Value Name:  MaxDisconnectionTime<br>Type:  REG_DWORD<br>Value:  0x0000ea60 (60000) | the registry value exists and is configured as specified | |
| 192 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Subkey:  \Software\Policies\Microsoft\Windows NT\Terminal Services\<br>Value Name:  MaxIdleTime<br>Type:  REG_DWORD<br>Value:  0x000dbba0 (900000) or less but not 0 | the following registry value exists and its value is set to 0 or less than 15 minutes | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 193 | Analyze the system using the Security Configuration and Analysis snap-in. Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\CurrentControlSet\Services\LanManServer\Parameters\<br>Value Name:  EnableForcedLogoff<br>Value Type:  REG_DWORD<br>Value:  1 | the value for “Microsoft Network Server: Disconnect Clients When Logon Hours Expire” is set to “Enabled” | |
| 194 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies >> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SYSTEM\CurrentControlSet\Services\LanManServer\Parameters\<br>Value Name:  autodisconnect<br>Value Type:  REG_DWORD<br>Value:  0x0000000f (15) (or less) | the value for "Microsoft Network Server: Amount of idle time required before suspending session" is set to "15" minutes or less | |
| **Test 115 SC-11 Trusted Path: The information system establishes a trusted communications path between the user and the following security functions of the system: [Assignment: organization-defined security functions to include at a minimum, information system authentication and reauthentication]. NSS Defined Value [], AF Defined Value . . . at a minimum, information system authentication and reauthentication.** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 195 | Review trusted path policies and procedures | . . . at a minimum, information system authentication and re-authentication | |
| **Test 116 SC-13 Use Of Cryptography: The information system implements required cryptographic protections using cryptographic modules that comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. NSS Defined Value [], AF Defined Value []** | | | |
| 196 | Analyze the system using the Security Configuration and Analysis snap-in.<br>Expand the Security Configuration and Analysis tree view.<br>Navigate to Local Policies -> Security Options.<br>The policy referenced configures the following registry value:<br>Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \System\ CurrentControlSet\Control\Lsa\ FIPSAlgorithmPolicy\<br>Value Name: Enabled<br>Value Type: REG_DWORD<br>Value: 1 | the value for “System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing” is set to “Enabled”<br>Warning: Clients with this setting enabled will not be able to communicate via digitally encrypted or signed protocols with servers that do not support these algorithms. Both the browser and web server must be configured to use TLS; the browser will not be able to connect to a secure site. | |
| **Test 117 SC-13 (3) Use Of Cryptography: The organization employs, at a minimum, FIPS-validated cryptography to protect information when such information must be separated from individuals who have the necessary clearances yet lack the necessary access approvals. NSS Defined Value [], AF Defined Value []** | | | |
| 197 | Review use of cryptography | | |
| **Test 118 SC-14 Public Access Protections: The information system protects the integrity and availability of publicly available information and applications. NSS Defined Value [], AF Defined Value []** | | | |
| 198 | Review public access protections | | |
| **Test 119 SC-15 Collaborative Computing Devices: The information system: a. Prohibits remote activation of collaborative computing devices with the following exceptions: [Assignment: organization-defined exceptions where remote activation is to be allowed]; and b. Provides an explicit indication of use to users physically present at the devices. NSS Defined Value a. Remote activation of centrally managed dedicated VTC Suites located in approved VTC locations, AF Defined Value []** | | | |
| 199 | Review collaborative computing devices policies and procedures | Remote activation of centrally managed dedicated VTC Suites located in approved VTC locations | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 120 SC-15 (1) Collaborative Computing Devices: The information system provides physical disconnect of collaborative computing devices in a manner that supports ease of use. NSS Defined Value [], AF Defined Value []** | | | |
| 200 | Review collaborative computing devices | | |
| **Test 121 SC-15 (2) Collaborative Computing Devices: The information system or supporting environment blocks both inbound and outbound traffic between instant messaging clients that are independently configured by end users and external service providers. NSS Defined Value [], AF Defined Value []** | | | |
| 201 | If an Instant Messaging client is installed, ask the SA if it has access to any public domain IM servers. | No public domain access | |
| **Test 122 SC-15 (3) Collaborative Computing Devices: The organization disables or removes collaborative computing devices from information systems in [Assignment: organization-defined secure work areas]. NSS Defined Value [], AF Defined Value . . . areas not approved for collaborative computing devices.** | | | |
| 202 | Review collaborative computing devices policies and procedures | . . . areas not approved for collaborative computing devices. | |
| **Test 123 SC-17 Public Key Infrastructure Certificates: The organization issues public key certificates under an [Assignment: organization defined certificate policy] or obtains public key certificates under an appropriate certificate policy from an approved service provider. NSS Defined Value [], AF Defined Value . . . DNI or DoD certificate policy, as appropriate** | | | |
| 203 | Review public key infrastructure certificates | | |
| **Test 124 SC-18 Mobile Code: The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 204 | Review mobile code | No mobile code | |
| **Test 125 SC-18 (1) Mobile Code: The information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary. NSS Defined Value [], AF Defined Value []** | | | |
| 205 | Review mobile code | No mobile code | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 126 SC-18 (2) Mobile Code: The organization ensures the acquisition, development, and/or use of mobile code to be deployed in information systems meets [Assignment: organization-defined mobile code requirements]. NSS Defined Value (a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.**<br>**(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.**<br>**(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.**<br>**(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).**<br>**(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used., AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 206 | Review mobile code | (a) Emerging mobile code technologies that have not undergone a risk assessment and been assigned to a Risk Category by the CIO are not used.<br>(b) Category 1 mobile code is signed with a code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited.<br>(c) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, and network connections to other than the originating host) may be used.<br>(d) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNet, SSL connection, S/MIME, code is signed with an approved code signing certificate).<br>(e) Category 3 (mobile code having limited functionality, with no capability for unmediated access to the services and resources of a computing platform) mobile code may be used. | |
| **Test 127 SC-18 (3) Mobile Code: The information system prevents the download and execution of prohibited mobile code. NSS Defined Value [], AF Defined Value []** | | | |
| 207 | Review mobile code | | |
| **Test 128 SC-18 (4) Mobile Code: The information system prevents the automatic execution of mobile code in [Assignment: organization-defined software applications] and requires [Assignment: organization-defined actions] prior to executing the code. NSS Defined Value . . . e-mail . . . prompting the user, AF Defined Value []** | | | |
| 208 | Review mobile code | . . . e-mail<br>. . . prompting the user | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 129 SC-19 Voice Over Internet Protocol: The organization: a. Establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; b. Authorizes, monitors, and controls the use of VoIP within the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 209 | Review voice over Internet Protocol | | |
| **Test 130 SC-20 Secure Name / Address Resolution Service (Authoritative Source): The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries. NSS Defined Value [], AF Defined Value []** | | | |
| 210 | Review Secure Name / Address Resolution Service (Authoritative Source) policies and procedures | Known IP address resolves to expected URL | |
| **Test 131 SC-20 (1) Secure Name / Address Resolution Service (Authoritative Source): The information system, when operating as part of a distributed, hierarchical namespace, provides the means to indicate the security status of child subspaces and (if the child supports secure resolution services) enable verification of a chain of trust among parent and child domains. NSS Defined Value [], AF Defined Value []** | | | |
| 211 | Review Secure Name / Address Resolution Service (Authoritative Source) policies and procedures | Known IP address resolves to expected URL | |
| **Test 132 SC-21 Secure Name / Address Resolution Service (Recursive Or Caching Resolver): The information system performs data origin authentication and data integrity verification on the name/address resolution responses the system receives from authoritative sources when requested by client systems. NSS Defined Value [], AF Defined Value []** | | | |
| 212 | Review Secure Name / Address Resolution Service (Authoritative Source) policies and procedures | Known IP address resolves to expected URL | |
| **Test 133 SC-21 (1) Secure Name / Address Resolution Service (Recursive Or Caching Resolver): The information system performs data origin authentication and data integrity verification on all resolution responses whether or not local clients explicitly request this service. NSS Defined Value [], AF Defined Value []** | | | |
| 213 | Review Secure Name / Address Resolution Service (Authoritative Source) policies and procedures | Known IP address resolves to expected URL | |
| **Test 134 SC-22 Architecture And Provisioning For Name / Address Resolution Service: The information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation. NSS Defined Value [], AF Defined Value []** | | | |
| 214 | Review Architecture And Provisioning For Name / Address Resolution Service | | |
| **Test 135 SC-23 Session Authenticity: The information system provides mechanisms to protect the authenticity of communications sessions. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 215 | Review Session Authenticity | | |
| **Test 136 SC-23 (1) Session Authenticity: The information system invalidates session identifiers upon user logout or other session termination. NSS Defined Value [], AF Defined Value []** | | | |
| 216 | Review Session Authenticity | Successful login and logout of session with no information remaining in the login box | |
| **Test 137 SC-23 (2) Session Authenticity: The information system provides a readily observable logout capability whenever authentication is used to gain access to web pages. NSS Defined Value [], AF Defined Value []** | | | |
| 217 | Review Session Authenticity | System does not have the capability to access web pages. | |
| **Test 138 SC-23 (3) Session Authenticity: The information system generates a unique session identifier for each session and recognizes only session identifiers that are system-generated. NSS Defined Value [], AF Defined Value []** | | | |
| 218 | Review Session Authenticity | | |
| **Test 139 SC-23 (4) Session Authenticity: The information system generates unique session identifiers with [Assignment: organization-defined randomness requirements]. NSS Defined Value [], AF Defined Value . . . randomly generated session identifier length of at least 128 bits** | | | |
| 219 | Review session authenticity policies and procedures | . . . randomly generated session identifier length of at least 128 bits | |
| **Test 140 SC-24 Fail In Known State: The information system fails to a [Assignment: organization-defined known-state] for [Assignment: organization-defined types of failures] preserving [Assignment: organization-defined system state information] in failure. NSS Defined Value (1) . . . known secure state (2) . . . all types of failures (3) . . . information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes . . ., AF Defined Value []** | | | |
| 220 | Review fail in known state policies and procedures | (1). . . known secure state (2). . . all types of failures (3). . . information necessary to determine cause of failure and to return to operations with least disruption to mission/ business processes . . . | |
| **Test 141 SC-28 Protection Of Information At Rest: The information system protects the confidentiality and integrity of information at rest. NSS Defined Value [], AF Defined Value []** | | | |
| 221 | Ask the SA if a root kit check tool is run on the system weekly. | A root kit check is run weekly. | |
| **Test 142 SC-32 Information System Partitioning: The organization partitions the information system into components residing in separate physical domains (or environments) as deemed necessary. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 222 | Ask the SA if this is an NMS server. If it is an NMS server, then ask what other applications run on it. | If NMS, ONLY used for network management software and DBMS software used only for the storage and inquiry of NMS data | |
| 223 | Ask the SA if the system boots from removable media. If so, ask if the boot media is stored in a secure container when not in use. | Media stored in a secure container | |
| 224 | Review the system architecture, drawings and system documentation. | The system is separated into physically separate domains where appropriate and the information system utilizes logical separation via zones for additional separation within the system. | |
| **Test 143 SI-3 (2) Malicious Code Protection: The information system automatically updates malicious code protection mechanisms (including signature definitions). NSS Defined Value [], AF Defined Value []** | | | |
| 225 | Verify an antivirus program is running; open the program to verify the .dat files are current | The .dat files are newer than 7 days old | |
| **Test 144 SI-3 (3) Malicious Code Protection: The information system prevents non-privileged users from circumventing malicious code protection capabilities. NSS Defined Value [], AF Defined Value []** | | | |
| 226 | Review Malicious Code Protection | | |
| **Test 145 SI-3 (5) Malicious Code Protection: The organization does not allow users to introduce removable media into the information system. NSS Defined Value [], AF Defined Value []** | | | |
| 227 | Interview site personnel and review local site policies to determine what policy and countermeasures are in place to prevent users from using removable media on the system | Site policy explicitly denies the use of removable media on the system. | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 146 SI-4 Information System Monitoring: The organization: a. Monitors events on the information system in accordance with [Assignment: organization-defined monitoring objectives] and detects information system attacks; c. Deploys monitoring devices: (i) strategically within the information system to collect organization-determined essential information; and (ii) at ad hoc locations within the system to track specific types of transactions of interest to the organization; d. Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and e. Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. NSS Defined Value [], AF Defined Value a. [ORGANIZATION] objectives**<br>**SI-4 (1) Information System Monitoring: The organization interconnects and configures individual intrusion detection tools into a system-wide intrusion detection system using common protocols. NSS Defined Value [], AF Defined Value []**<br>**SI-4 (2) Information System Monitoring: The organization employs automated tools to support near real-time analysis of events. NSS Defined Value [], AF Defined Value []** | | | |
| 228 | Verify the hbss agent is running. | The service should be present. | |
| 229 | Verify the Agent Handler server has met registered DoD ports, protocols, and services (PPS) requirements | Verify the following ports are registered:<br>Agent-to-server: MCAFEE-HBSS-SPIPE HTTP and MCAFEE-HBSS-SPIPE HTTPS TCP 80 / MCAFEE-HBSS-SPIPE HTTP and MCAFEE-HBSS-SPIPE HTTPS TCP 443<br>Agent wake-up: MCAFEE-HBSS-SPIPE HTTP and MCAFEE-HBSS-SPIPE HTTPS TCP 591<br>Agent Handler-to-ePO: MCAFEE-HBSS-SPIPE HTTP and MCAFEE-HBSS-SPIPE HTTPS TCP 8443<br>Agent Handler-to-SQL Database: MCAFEE-HBSS-SPIPE HTTP and MCAFEE-HBSS-SPIPE HTTPS TCP 1443 | |
| **Test 149 SI-4 (4) Information System Monitoring: The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions. NSS Defined Value [], AF Defined Value []** | | | |
| 230 | Verify there are deny-by-default access control lists (ACLs), both inbound and outbound, within the perimeter protecting the hbss Agent Handler server. | there is deny-by-default ACLs, either inbound or outbound, within the perimeter protecting the Agent Handler server | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 150 SI-4 (5) Information System Monitoring: The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators]. NSS Defined Value [], AF Defined Value . . . audit records, alerts from malicious code detection mechanisms, intrusion detection or prevention mechanisms, boundary protection mechanisms such as firewalls, gateways, and routers.** | | | |
| 231 | Review information system monitoring policies and procedures | . . . audit records, alerts from malicious code detection mechanisms, intrusion detection or prevention mechanisms, boundary protection mechanisms such as firewalls, gateways, and routers. | |
| **Test 151 SI-4 (6) Information System Monitoring: The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. NSS Defined Value [], AF Defined Value []** | | | |
| 232 | Examine the network topology and verify the local network IDS exists. | there is local network IDS in place | |
| **Test 152 SI-4 (7) Information System Monitoring: The information system notifies [Assignment: organization-defined list of incident response personnel (identified by name and/or by role)] of suspicious events and takes [Assignment: organization-defined list of least-disruptive actions to terminate suspicious events]. NSS Defined Value [], AF Defined Value 1 . . . incident response personnel . . . 2 . . . the least disruptive action to terminate suspicious events as determined appropriate for the individual system.** | | | |
| 233 | Review information system monitoring policies and procedures | (1). . . incident response personnel<br>(2). . . the least disruptive action to terminate suspicious events as determined appropriate for the individual system. | |
| **Test 153 SI-4 (11) Information System Monitoring: The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. NSS Defined Value [], AF Defined Value []** | | | |
| 234 | Interview (ORGANIZATION) network administrators about outbound communications monitoring. | The ORGANIZATION analyzes outbound communications at the external boundary of the system. | |
| **Test 154 SI-4 (15) Information System Monitoring: The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks. NSS Defined Value [], AF Defined Value []** | | | |
| 235 | Review information system monitoring policies and procedures | No wireless networks deployed. | |
| **Test 155 SI-4 (16) Information System Monitoring: The organization correlates information from monitoring tools employed throughout the information system to achieve organization-wide situational awareness. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 236 | Review information system monitoring | | |
| **Test 156 SI-6 Security Functionality Verification: The information system verifies the correct operation of security functions [Selection (one or more): [Assignment: organization-defined system transitional states]; upon command by user with appropriate privilege; periodically every [Assignment: organization-defined time-period]] and [Selection (one or more): notifies system administrator; shuts the system down; restarts the system; [Assignment: organization-defined alternative action(s)]] when anomalies are discovered. NSS Defined Value 3 . . . notifies system administrator . . ., AF Defined Value 1 . . . upon system startup and/or restart**<br>**2 . . . at least every 90 days** | | | |
| 237 | Check virus scanning and review security functionality verification policies and procedures | (1). . . upon system startup and/or restart<br>(2). . . at least every 90 days<br>(3). . . notifies system administrator | |
| **Test 157 SI-6 (1) Security Functionality Verification: The information system provides notification of failed automated security tests. NSS Defined Value [], AF Defined Value []** | | | |
| 238 | Review security functionality verification | | |
| **Test 158 SI-6 (3) Security Functionality Verification: The information system provides automated support for the management of distributed security testing. NSS Defined Value [], AF Defined Value []** | | | |
| 239 | Review security functionality verification | | |
| **Test 159 SI-8 Spam Protection: The organization: a. Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and b. Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures. NSS Defined Value [], AF Defined Value []** | | | |
| 240 | Review spam protection | | |
| **Test 160 SI-8 (1) Spam Protection: The organization centrally manages spam protection mechanisms. NSS Defined Value [], AF Defined Value []** | | | |
| 241 | (N/A since mail is not used on the system and throughout the ORGANIZATION enterprise) | | |
| **Test 161 SI-8 (2) Spam Protection: The information system automatically updates spam protection mechanisms (including signature definitions). NSS Defined Value [], AF Defined Value []** | | | |
| 242 | (N/A since mail is not used on the system and throughout the ORGANIZATION enterprise) | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| **Test 162 SI-9 Information Input Restrictions: The organization restricts the capability to input information to the information system to authorized personnel. NSS Defined Value [], AF Defined Value []** | | | |
| 243 | Interview site personnel and read through the site access control policy and access control list. | Checks and balances are in place to ensure only authorized personnel have access to the system. | |
| 244 | Attempt to access the system without credentials | You cannot access the system without access control credentials. | |
| **Test 163 SI-10 Information Input Validation: The information system checks the validity of information inputs. NSS Defined Value [], AF Defined Value []** | | | |
| 245 | Review information input validation | | |
| **Test 164 SI-11 Error Handling: The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel. NSS Defined Value [], AF Defined Value b. . . sensitive or potentially harmful information** | | | |
| 246 | Verify the Start Type and Status of the Windows Error Reporting Service. Run "Services.msc". | the Windows Error Reporting Service has a Status of "Started" and a Start Type of "Automatic" | |
| 247 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: Disabled<br>Type: REG_DWORD<br>Value: 0 | the registry value exists and is configured as specified | |
| 248 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: LoggingDisabled<br>Type: REG_DWORD<br>Value: 0 | the registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 249 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: DontSendAdditionalData<br>Type: REG_DWORD<br>Value: 0 | the registry value exists and is configured as specified | |
| 250 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: DontShowUI<br>Type: REG_DWORD<br>Value: 1 | the registry value exists and is configured as specified | |
| 251 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: CorporateWerServer<br>Type: REG_SZ<br>Value: " " (A single BLANK character to store the data on the system or the error reporting server name or IP address to forward the data to.) | the registry value exists and is configured as specified | |
| 252 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: DisableArchive<br>Type: REG_DWORD<br>Value: 0 | the registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 253 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name:  ConfigureArchive<br>Type:  REG_DWORD<br>Value:  0x00000002 (2) | the registry value exists and is configured as specified | |
| 254 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name:  MaxArchiveCount<br>Type:  REG_DWORD<br>Value:  0x00000064 (100)  (or greater) | the registry value exists and is configured as specified | |
| 255 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name:  DisableQueue<br>Type:  REG_DWORD<br>Value:  0 | the registry value exists and is configured as specified | |
| 256 | Registry Hive:  HKEY_LOCAL_MACHINE<br>Registry Path:  \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name:  ForceQueue<br>Type:  REG_DWORD<br>Value:  1 | the registry value exists and is configured as specified | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 257 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: MaxQueueCount<br>Type: REG_DWORD<br>Value: 0x00000032 (50) (or greater) | the registry value exists and is configured as specified | |
| 258 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\<br>Value Name: QueuePesterInterval<br>Type: REG_DWORD<br>Value: 1 | the registry value exists and is configured as specified | |
| 259 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\Consent\<br>Value Name: DefaultConsent<br>Type: REG_DWORD<br>Value: 0x00000004 (4) | the registry value exists and is configured as specified | |
| 260 | Registry Hive: HKEY_LOCAL_MACHINE<br>Registry Path: \SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting\Consent\<br>Value Name: DefaultOverrideBehavior<br>Type: REG_DWORD<br>Value: 1 | the registry value exists and is configured as specified | |
| **Test 165 SI-12 Information Output Handling And Retention: The organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. NSS Defined Value [], AF Defined Value []** | | | |

| Step | Step Description | Expected Results/Comments | P/F |
|---|---|---|---|
| 261 | Review information output handling and retention policies and procedures | organization handles and retains both information within and output from the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements | |
| Notes: | | | |

## 4.2 Reporting

A final After Action Report (AAR) will be provided to all [ORGANIZATION] stakeholders within 30 days of completion of demonstration execution.