Compliance Self Test Plan for GENERIC, Linux, version 2016

09 NOV2023

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 Linux 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 [OPERATIONAL] 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 LINUX 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.

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 TEST SCENARIO: 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. TEST SETUP: 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). 2. Once logged on, the test executioner will open a shell by clicking on Hosts and selecting Console. 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	Check the system for unnecessary user accounts. # more /etc/passwd	No unnecessary accounts; examples of unnecessary accounts include games, news, gopher, ftp, and lp, and may also include ADMIN and TEST accounts.	
2	Check /etc/pam.d/su uses pam_wheel. # grep pam_wheel /etc/pam.d/su	pam_wheel is present	
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 []			

Step	Step Description	Expected Results/Comments	P/F
3	Review site account establishment and management processes and interview account managers	Processes should include: a. Identification of account types (i.e., individual, group, system, application, guest/anonymous, and temporary) b. Establishing conditions for group membership c. Identifying authorized users of the information system and specifying access privileges d. Requiring appropriate approvals for requests to establish accounts e. Establishing, activating, modifying, disabling, and removing accounts f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts 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 h. Deactivating: - temporary accounts that are no longer required - accounts of terminated or transferred users i. Granting access to the system based on: - valid access authorization - intended system usage - other attributes as required by the organization or associated missions/business functions j. Reviewing accounts during some defined frequency	
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 []			

Step	Step Description	Expected Results/Comments	P/F
4	Check the date in the "last" log to verify it is within the last 90 days or the maximum numbers of days set by the site if more restrictive. The passwd command can also be used to list a status for an account. For example, the following may be used to provide status information on each local account: NOTE: The following must be done in the BASH shell. # cut -d: -f1 /etc/passwd | xargs -n1 passwd -S	No inactive account is not disabled via an entry in the password field in the /etc/passwd or /etc/shadow (or equivalent), check the /etc/passwd file to check if the account has a valid shell.	

5	verify the "INACTIVE" setting, run the following command:
	
	# grep "INACTIVE" /etc/default/useradd
		indicate the "INACTIVE" configuration option is set to an appropriate integer as shown in the example below:
		
		# grep "INACTIVE" /etc/default/useradd
		INACTIVE=90	

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 []			
6	Determine if execution of the useradd and groupadd executable are audited. # auditctl -l | egrep '(useradd| groupadd)' Determine if /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow are audited for appending. # auditctl -l | egrep '(/etc/passwd|/etc/shadow|/etc/group|/etc/gshadow)' Determine if execution of the passwd executable is audited. # auditctl -l | grep /usr/bin/passwd Determine if execution of the userdel and groupdel executable are audited. # auditctl -l | egrep '(userdel| groupdel)'	either useradd or groupadd are listed with a permissions filter of at least 'x'	

Step	Step Description	Expected Results/Comments	P/F
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	Check if the system requires a password for entering single-user mode. # grep ':S:' /etc/inittab	Password is required	
9	On systems with a BIOS or system controller, verify a supervisor or administrator password is set. Check the "/boot/grub/grub.conf" or "/boot/grub/menu.lst" files. # more /boot/grub/menu.lst Check for a password configuration line, such as: password --md5 <password-hash>	Password is required	
10	Check GRUB for password configuration. Procedure: Check the /boot/grub/grub.conf or /boot/grub/menu.lst files. # grep "password" /boot/grub/grub.conf /boot/grub/menu.lst Check for a password configuration line, such as: password --md5 <password-hash>	Configuration line found	
11	# etc/grub.conf	GRUB	
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 []			

Step	Step Description	Expected Results/Comments	P/F
12	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.	
13	# umask etc/login.defs	027 (750)	
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 []			
14	Verify the system does not accept source-routed IPv4 packets. Procedure: # grep [01] /proc/sys/net/ipv4/conf/*/accept_source_route|egrep "default|all"	all of the returned lines end with "0"	
15	Verify the system does not respond to ICMP TIMESTAMP_REQUESTs Procedure: # grep "timestamp" /etc/sysconfig/iptables	This should return entries for "timestamp-reply" and "timestamp_request". Both should end with "-j DROP', and both should exist.	
16	Verify the system does not respond to ICMP ECHO_REQUESTs set to broadcast addresses. Procedure: # cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts	Result is 1	
17	Verify the system does not respond to ICMP TIMESTAMP_REQUESTs set to broadcast addresses. Procedure: # cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts	Result is 1	
18	Verify the system does not use proxy ARP. # grep [01] /proc/sys/net/ipv4/conf/*/proxy_arp|egrep "default|all"	all of the resulting lines end with "0"	

Step	Step Description	Expected Results/Comments	P/F
19	Verify the system does not accept IPv4 ICMP redirect messages. # grep [01] /proc/sys/net/ipv4/conf/*/accept_redirects|egrep "default|all"	all of the resulting lines end with "0"	
20	Verify the system does not send IPv4 ICMP redirect messages. # grep [01] /proc/sys/net/ipv4/conf/*/send_redirects|egrep "default|all"	all of the resulting lines end with "0"	
21	Verify the system is not configured for bridging. # ls /proc/sys/net/bridge No directory exists # lsmod | grep '^bridge '	No results returned	
22	Verify the Bluetooth protocol handler is prevented from dynamic loading. # grep 'install bluetooth /bin/true' /etc/modprobe.conf /etc/modprobe.d/*	results returned to verify preventive loading	
23	# grep disable /etc/xinetd.d/finger	the finger service is disabled	
24	Verify the IPv6 protocol handler is prevented from dynamic loading. # grep 'install ipv6 /bin/true' /etc/modprobe.conf /etc/modprobe.d/*	No IPv6 protocol	
25	Check the system for any active 6to4 tunnels without specific remote addresses. # ip tun list | grep "remote any" | grep "ipv6/ip"	No results returned	
26	Verify the Miredo service is not running. # ps ax | grep miredo | grep -v grep	Not running	
27	Check for any IP tunnels. # ip tun list # ip -6 tun list	No tunnels listed	
28	Verify the system is configured to ignore IPv6 ICMP redirect messages. # cat /proc/sys/net/ipv6/conf/all/accept_redirects	the returned value is "0"	

Step	Step Description	Expected Results/Comments	P/F
29	Determine if the system is configured to forward IPv6 source-routed packets. Procedure: # egrep "net.ipv6.conf.*forwarding" /etc/sysctl.conf	the returned value is "0"	
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 []			
30	Check the permissions on the files or scripts executed from system startup scripts to see if they are world-writable. Create a list of all potential run command level scripts. # ls -l /etc/init.d/* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 -d " " OR # ls -l /sbin/init.d/* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 -d " " Create a list of world writeable files. # find / -perm -002 -type f >> worldWriteableFileList Determine if any of the world writeable files in worldWriteableFileList are called from the run command level scripts. Note: Depending upon the number of scripts vs world writeable files, it may be easier to inspect the scripts manually. # more `ls -l /etc/init.d/* | tr '\ 011' ' ' | tr -s ' ' | cut -f 9,9 -d " "` OR # more `ls -l /sbin/init.d/* | tr '\ 011' ' ' | tr -s ' ' | cut -f 9,9 -d " "`	No system startup script executes any file or script that is world-writable	

Step	Step Description	Expected Results/Comments	P/F
31	If /etc/shells exists, check the group ownership of each shell referenced. # cat /etc/shells | xargs -n1 ls -l Otherwise, check any shells found on the system. # find / -name "*sh" | xargs -n1 ls -l	a shell has a mode less permissive than 0755	
32	Look in the root account home directory for a .mozilla directory. If there is one, verify with the root users and the IAO the intent of the browsing.	the browsing is limited to authorized local services administration	
33	Verify the ownership of files referenced within the sendmail aliases file. Procedure: # more /etc/aliases Examine the aliases file for any utilized directories or paths. # ls -lL <directory or file path> Check the owner for any paths referenced.	the file or parent directory is owned by root	
34	Check the shell for the anonymous FTP account. Procedure: # grep "^ftp" /etc/passwd	the seventh field is not empty (the entry ends with a ':') or if the seventh field does not contain one of the following: /bin/false /dev/null /usr/bin/false /bin/true /sbin/nologin	
35	Check the mode of the TFTP daemon. Procedure: # grep "server " /etc/xinetd.d/tftp # ls -lL <in.tftpd binary>	he mode of the file is less permissive than 0755	
36	Determine if the TFTP daemon is active. # chkconfig --list | grep tftp	TFTP is found enabled ("on") and is documented using site-defined procedures	

Step	Step Description	Expected Results/Comments	P/F
37	Check the output of the "xhost" command from an X terminal. Procedure: # xhost The output may report access control is enabled (and possibly lists the hosts able to receive X window logins). Note: It may be necessary to define the display if the command reports it cannot open the display. Procedure: $ DISPLAY=MachineName:0.0; export DISPLAY MachineName may be replaced with an Internet Protocol Address. Repeat the check procedure after setting the display.	he xhost command returns a line indicating access control is enabled	
38	Perform the following to check for unnecessary privileged accounts: # grep "^shutdown" /etc/passwd # grep "^halt" /etc/passwd # grep "^reboot" /etc/passwd	No unnecessary privileged accounts exist	
39	Determine if an NFS server is running on the system by: # ps -ef |grep nfsd If an NFS server is running, confirm it is not configured with the insecure_locks option by: # exportfs -v	The output is not like the following; /misc/export speedy.example.com(rw,insecure_locks)	

Step	Step Description	Expected Results/Comments	P/F
40	Verify the /etc/passwd file is owned by root. # ls -l /etc/passwd Check the group ownership of the passwd file. Procedure: # ls -lL /etc/passwd	the file is owned by root he file is group-owned by root, bin or sys /etc/passwd has a mode less permissive than 0644 the permissions do not include a '+', the file does not have an extended ACL the file has an extended ACL and it has been documented with the IAO	
41	Verify the /etc/group file is owned by root. # ls -l /etc/group Check the group ownership of the group file. Procedure: # ls -lL /etc/group	the file is owned by root he file is group-owned by root, bin or sys /etc/passwd has a mode less permissive than 0644 the permissions do not include a '+', the file does not have an extended ACL the file has an extended ACL and it has been documented with the IAO	
42	Verify the /etc/shadow file is owned by root. # ls -l /etc/shadow Check the group ownership of the shadow file. Procedure: # ls -lL /etc/shadow	the file is owned by root he file is group-owned by root, bin or sys /etc/passwd has a mode less permissive than 0400 the permissions do not include a '+', the file does not have an extended ACL the file has an extended ACL and it has been documented with the IAO	

Step	Step Description	Expected Results/Comments	P/F
43	Use pwck to verify home directory assignments are present. # pwck	All users are assigned a home directory No user's assigned home directory does not exist	
44	Check the /etc/group file for password hashes. # cut -d : -f 2 /etc/group | egrep -v '^(x|!)$'	No password hashes are returned	
45	Check the home directory mode of each user in /etc/passwd. Procedure: # cut -d: -f6 /etc/passwd|sort|uniq| xargs -n1 ls -ld	user home directory's mode is less permissive than 0750 Note: Application directories are allowed and may need 0755 permissions (or greater) for correct operation.	
46	Verify user home directories have no extended ACLs. # cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld	the permissions do not include a '+', if so, the file has an extended ACL	
47	Check the ownership of each user home directory listed in the /etc/passwd file. Procedure: # cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld	All user home directory is owned by the assigned user	
48	Check the group ownership for each user in the /etc/passwd file. Procedure: # cut -d : -f 6 /etc/passwd | xargs -n1 ls -ld	All user home directory is group-owned by the assigned user's primary group Home directories for application accounts requiring different group ownership must be documented using site-defined procedures.	
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 []			

Step	Step Description	Expected Results/Comments	P/F
49	Check the pam_tally configuration. # more /etc/pam.d/system-auth Confirm the following line is configured, before any "auth sufficient" lines: auth required pam_tally2.so deny=3	The line is found	
50	Check the value of the FAIL_DELAY variable and the ability to use it. Procedure: # grep FAIL_DELAY /etc/login.defs	the value exists and is 4 or greater than 4	
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 []			
51	Check for the use of pam_faildelay. # grep pam_faildelay /etc/pam.d/system-auth* If pam_faildelay is present only in /etc/pam.d/system-auth-ac: ensure that /etc/pam.d/system-auth includes /etc/pam.d/system-auth-ac. #grep system-auth-ac /etc/pam.d/system-auth	pam_faildelay.so module is present This should return: auth include system-auth-ac account include system-auth-ac password include system-auth-ac session include system-auth-ac /etc/pam.d/system-auth-ac should only be included by /etc/pam.d/system-auth. All other pam files should include /etc/pam.d/system-auth. pam_faildelay is defined in /etc/pam.d/system-auth either directly or through inclusion of system-auth-ac	

Step	Step Description	Expected Results/Comments	P/F
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
52	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: "You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -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. -At any time, the USG may inspect and seize data stored on this IS. -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. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy. -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. "	
53	Verify the SSH daemon is configured for logon warning banners. Follow Step 46.	Same output as Step 46.	

Step	Step Description	Expected Results/Comments	P/F
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 []			
54	Check that pam_lastlog is used and not silent, or that the SSH daemon is configured to display last login information. # grep pam_lastlog /etc/pam.d/sshd # grep -i PrintLastLog /etc/ssh/sshd_config PrintLastLog is not present in the configuration, is the default setting	pam_lastlog is present, and does not have the "silent" option PrintLastLog is present in the configuration and set to "yes" (case insensitive)	
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 []			
55	For the Gnome screen saver, check the idle_activation_enabled flag. Procedure: # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --get /apps/gnome-screensaver/idle_activation_enabled	return "true"	
56	For the Gnome screen saver, check the idle_delay setting. Procedure: # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --get /apps/gnome-screensaver/idle_delay	return 15 or less	

Step	Step Description	Expected Results/Comments	P/F
57	For the Gnome screen saver, check the lock_enabled flag. Procedure: # gconftool-2 --direct --config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory --get /apps/gnome-screensaver/lock_enabled	return "true"	
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 []			
58	Review session lock visual	The adherence to the control is visible	
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 []			
59	Determine if a publicly-viewable pattern is displayed during a session lock. Some screensaver themes available but not included in the RHEL distribution use a snapshot of the current screen as a graphic. This theme does not qualify as a publicly-viewable pattern.	the session lock pattern is publicly-viewable	
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 []			
60	Check if the 'anonuid' and 'anongid' options are set correctly for exported file systems. List exported filesystems: # exportfs -v	Each of the exported file systems should include an entry for the 'anonuid=' and 'anongid=' options set to "-1" or an equivalent (60001, 65534, or 65535).	
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 []			
61	Review remote access authorization policy and procedures.	Remote access is documented in policy and procedures	

Step	Step Description	Expected Results/Comments	P/F
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 []			
62	Determine if auditing is enabled. # ps -ef |grep auditd	the auditd process is found	
63	Check /etc/syslog.conf and verify the auth facility is logging both the notice and info level messages by using one of the procedures below. # grep "auth.notice" /etc/syslog.conf # grep "auth.info" /etc/syslog.conf OR # grep 'auth.*' /etc/syslog.conf	auth.* is found, and either auth.notice or auth.info is found	
64	The system's access control program must log each system access attempt. # more /etc/syslog.conf	syslog is configured to log events by TCPD	
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 []			
65	Check to see if rshd is configured to run on startup. Procedure: # grep disable /etc/xinetd.d/rsh	/etc/xinetd.d/rsh does not exist and rsh is disabled	
66	Check the rlogind configuration. # cat /etc/xinetd.d/rlogin	the file exists and contains "disable = yes"	
67	Verify the SNMP daemon uses SHA for SNMPv3 users. Procedure: Examine the default install location /etc/snmp/snmpd.conf or: # find / -name snmpd.conf # grep -v '^#' <snmpd.conf file> | grep -i createuser | grep -vi SHA	Nothing returned	

Step	Step Description	Expected Results/Comments	P/F
68	Verify the SNMP daemon uses AES for SNMPv3 users. Procedure: Examine the default install location /etc/snmp/snmpd.conf or: # find / -name snmpd.conf # grep -v '^#' <snmpd.conf file> | grep -i createuser | grep -vi AES	Nothing returned	
69	Check the SSH daemon configuration for allowed ciphers. # grep -i ciphers /etc/ssh/sshd_config | grep -v '^#'	Returned lines starting with "3des" or "aes"	
70	Check the SSH daemon configuration for allowed MACs. Procedure: # grep -i macs /etc/ssh/sshd_config | grep -v '^#'	Returned lines with hmac-sha1 or a better hmac algorithm that is on the FIPS 140-2 approved list	

Step	Step Description	Expected Results/Comments	P/F
71	To check to see if the system is an LDAP server, verify LDAP is running on the system: # ps -ef | grep ldap Find out which LDAP is used (if not determined via the command above). # rpm -qa | grep ldap If using nssldap: # grep base /etc/ldap.conf Check to see if the base is set to something besides the default of "dc=example,dc=com". If using openldap: # grep suffix /etc/openldap/slapd.conf Check whether the system is an LDAP client: # grep server /etc/ldap.conf # grep server /etc/openldap/ldap.conf Check whether the server option has an address other than the loopback, then check the nsswitch.conf file. # grep ldap /etc/nsswitch.conf Look for the following three lines: passwd: files ldap shadow: files ldap group: files ldap If all three files are not configured to look for an LDAP source, then the system is not using LDAP for authentication. Check if NSS LDAP is using TLS. # grep '^ssl start_tls' /etc/ldap.conf Check if NSS LDAP TLS is using only FIPS 140-2 approved cryptographic algorithms. # grep '^tls_ciphers' /etc/ldap.conf	Retuned lines use TLS Lines retuned contain only ciphers approved by FIPS 140-2, to include 3DES and AES	

Step	Step Description	Expected Results/Comments	P/F
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 []			
72	Ask the SA to identify which interfaces on the system are designated for management traffic. If all interfaces on the system are authorized for management traffic, this is not applicable. Check the SSH daemon configuration for listening network addresses. # grep -i Listen /etc/ssh/sshd_config | grep -v '^#'	returned 'Listen' configuration contains addresses designated for management traffic	
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 []			
73	Check /etc/securetty # more /etc/securetty	file exists and contains "console" or a single "tty" device	
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] **. . .other encrypted channel with blocking mode enabled**			
74	Review remote access policies and procedures	. . . privileged functions and security relevant information . . . Secure Shell [SSH], Virtual Private Networking [VPN] . . . other encrypted channel with blocking mode enabled	
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 []			
75	Review remote access authorization policy and procedures.	No wireless access allowed.	
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 []			
76	Review remote access control for mobile devices policy and procedures.	No mobile devices allowed.	

Step	Step Description	Expected Results/Comments	P/F
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 []			
77	Review use of external IS policy and procedures.	No external IS allowed.	
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 []			
78	Review user-based collaboration and information sharing	There are no automated systems for information sharing.	
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 []			
79	Determine if all logon attempts are being logged. Verify successful logins are being logged: # last -R | more	Return successful logins	
80	Verify if unsuccessful logons are being logged: # lastb -R | more	Return unsuccessful logins	

Step	Step Description	Expected Results/Comments	P/F
81	Check the log files to determine if access to the root account is being logged. Procedure: Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file. Examine /etc/syslog.conf or /etc/rsyslog.conf to confirm the location to which "authpriv" messages will be directed. The default syslog.conf or rsyslog.conf uses /var/log/messages and /var/log/secure but this needs to be confirmed. # grep @ /etc/syslog.conf Or: # grep @ /etc/rsyslog.conf If a line starting with "*.*" is returned then all syslog messages will be sent to system whose address appears after the "@". In this case syslog may or may not be configured to also log "authpriv" messages locally. # grep authpriv /etc/syslog.conf Or: # grep authpriv /etc/rsyslog.conf Try to "su -" and enter an incorrect password.	If any lines are returned which do not start with "#" the "authpriv" messages will be sent to the indicated files or remote systems. There should be records that indicate the authentication failure.	

Step	Step Description	Expected Results/Comments	P/F
82	Verify auditd is configured to audit failed file access attempts. There must be an audit rule for each of the access syscalls logging all failed accesses (-F success=0) or there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S creat" | grep -e "-F success=0" # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S creat" | grep -e "-F exit=-EPERM" # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S creat" | grep -e "-F exit=-EACCES"	an "-S creat" audit rule with "-F success" exists and separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "creat" exist	
83	Check the system audit configuration to determine if file and directory deletions are audited. # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "unlink"	Results returned contain "-S unlink"	
84	The message types that are always recorded to /var/log/audit/audit.log include LOGIN, USER_LOGIN, USER_START, and USER_END among others and do not need to be added to audit_rules. The log files /var/log/faillog and /var/log/lastlog must be protected from tampering of the login records. Procedure: #egrep "faillog|lastlog" /etc/audit/audit.rules|grep "-p (wa|aw)"	both /var/log/faillog and /var/log/lastlog entries exist	

Step	Step Description	Expected Results/Comments	P/F
85	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i " chmod "	"-S chmod"	
86	Determine if the init_module syscall is audited. # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "init_module"	"-S init_module"	
87	Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file. # grep cron /etc/syslog.conf Or: # grep cron /etc/rsyslog.conf	cron logging is configured	
88	Check the configured cron log file found in the cron entry of /etc/syslog.conf or /etc/rsyslog.conf (normally /var/log/cron). # ls -lL /var/log/cron	File exists and is younger than the last cron job	
89	Verify the system logs martian packets. # grep [01] /proc/sys/net/ipv4/conf/*/log_martians |egrep "default|all"	all of the resulting lines end with "1"	

Step	Step Description	Expected Results/Comments	P/F
90	Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file. Check /etc/syslog.conf or /etc/rsyslog.conf and verify the authpriv facility is logging both the "notice" and "info" priority messages. Procedure: For a given action all messages of a higher severity or "priority" are logged. The three lowest priorities in ascending order are "debug", "info" and "notice". A priority of "info" will include "notice". A priority of "debug" includes both "info" and "notice". Enter/Input for syslog: # grep "authpriv.debug" /etc/syslog.conf # grep "authpriv.info" /etc/syslog.conf # grep "authpriv\.*" /etc/syslog.conf Enter/Input for rsyslog: # grep "authpriv.debug" /etc/rsyslog.conf # grep "authpriv.info" /etc/rsyslog.conf # grep "authpriv\.*" /etc/rsyslog.conf	an "authpriv.*", "authpriv.debug", or "authpriv.info" entry is found	
91	Check the syslog configuration file for mail.crit logging configuration. Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file. Procedure: # grep "mail\." /etc/syslog.conf Or: #grep "mail\." /etc/syslog.conf	syslog is configured to log critical sendmail messages ("mail.crit" or "mail.*")	

Step	Step Description	Expected Results/Comments	P/F
92	The tcp_wrappers package is provided with the RHEL distribution. Other access control programs may be available but will need to be checked manually. Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file. Normally, tcpd logs to the mail facility in "/etc/syslog.conf" or "/etc/rsyslog.conf". Determine if syslog or rsyslog is configured to log events by tcpd. Procedure: # grep -E "(*.info|*.debug| authpriv.info|authpriv.debug| authpriv.*)" /etc/syslog.conf | grep –v '#' Or: # grep -E "(*.info|*.debug| authpriv.info|authpriv.debug| authpriv.*)" /etc/rsyslog.conf | grep –v '#'	entries exist there no "authpriv.info", "authpriv.debug", "authpriv.*" or "*.info" or "*.debug" not followed by "authpriv.none" If an alternate access control program is used, it should provide logging of access attempts	
93	Check that auditd is configured to audit failed file access attempts. There must be an audit rule for each of the access syscalls that logs all failed accesses (-F success=0) or there must both an "-F exit=-EPERM" and "-F exit=-EACCES" for each access syscall. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S open" | grep -e "-F success=0" # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S open" | grep -e "-F exit=-EPERM" # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -e "-S open" | grep -e "-F exit=-EACCES"	an "-S open" audit rule with "-F success" exists and separate rules containing "-F exit=-EPERM" and "-F exit=-EACCES" for "open" exist	

Step	Step Description	Expected Results/Comments	P/F
94	Check the system audit configuration to determine if file and directory deletions are audited. # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "rmdir"	Results contain "-S rmdir"	
95	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchmod"	"-S fchmod"	
96	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchmodat"	"-S fchmodat"	
97	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "chown" Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86_64): # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "chown32"	"-S chown" "-S chown32"	

Step	Step Description	Expected Results/Comments	P/F
98	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchown" Additionally, the following rule is required in systems supporting the 32-bit syscall table (such as i686 and x86_64): # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchown32"	"-S fchown" "-S fchown32"	
99	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fchownat"	"-S fchownat"	
100	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "lchown"	"-S lchown"	
101	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "setxattr"	"-S setxattr"	
102	Determine if the delete_module syscall is audited. # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "delete_module"	"-S delete_module"	

Step	Step Description	Expected Results/Comments	P/F
103	Determine if /sbin/insmod is audited. # cat /etc/audit/audit.rules | grep "/sbin/insmod" Determine if the /sbin/modprobe file is audited. # cat /etc/audit/audit.rules | grep "/sbin/modprobe" Determine if the /sbin/rmmod file is audited. # cat /etc/audit/audit.rules | grep "/sbin/rmmod"	Results start with "-w" and contain "-p x"	
104	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fsetxattr"	"-S fsetxattr"	
105	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "removexattr"	"-S removexattr"	
106	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "lremovexattr"	"-S lremovexattr"	
107	Check the system's audit configuration. Procedure: # cat /etc/audit/audit.rules | grep -e "-a exit,always" | grep -i "fremovexattr"	"-S fremovexattr"	

Step	Step Description	Expected Results/Comments	P/F
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 []			
108	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 []			
109	The /etc/xinetd.conf file and each file in the /etc/xinetd.d directory file should be examined for the following: Procedure: log_type = SYSLOG authpriv log_on_success = HOST PID USERID EXIT log_on_failure = HOST USERID	xinetd is running and logging is enabled	

Step	Step Description	Expected Results/Comments	P/F
110	Find if logging is applied to the ftp daemon. The procedure depends on the implementation of ftpd used by the system. Procedures: For vsftpd: If vsftpd is started by xinetd: #grep vsftpd /etc/xinetd.d/* This will indicate the xinetd.d startup file #grep server_args <vsftpd xinetd.d startup file> This will indicate the vsftpd config file used when starting through xinetd. If the line is missing then "/etc/vsftpd/vsftpd.conf", the default config file, is used. #grep xferlog_enable <vsftpd config file> If vsftp is not started by xinetd: #grep xferlog_enable /etc/vsftpd/vsftpd.conf For gssftp: Find if the -l option will be applied when xinetd starts gssftp # grep server_args /etc/xinetd.d/gssftp	"xferlog_enable" or “yes” Line exists and contains at least one -l	
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 . . .			

Step	Step Description	Expected Results/Comments	P/F
111	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.			
112	Verify the system is configured to forward all audit records to a remote server. If the system is not configured to provide this function, this is a finding. Procedure: Ensure the audit option for the kernel is enabled. # grep "audit" /boot/grub/grub.conf | grep -v "^#"	"audit=1" option specified	
113	Ensure the kernel auditing is active. # grep "active" /etc/audisp/plugins.d/syslog.conf | grep -v "^#"	"active" or set to "yes"	
114	Ensure all audit records are forwarded to a remote server. # grep "*.*" /etc/syslog.conf |grep "@" | grep -v "^#" (for syslog) or: # grep "*.*" /etc/rsyslog.conf | grep "@" | grep -v "^#" (for rsyslog)	Lines exist	

Step	Step Description	Expected Results/Comments	P/F
115	Check the syslog configuration file for remote syslog servers. Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file. # grep '@' /etc/syslog.conf | grep -v '^#' Or: # grep '@' /etc/rsyslog.conf | grep -v '^#'	Line returned	
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 []			
116	Review audit storage capacity policy and procedures.	Storage capacity is allocated	
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			
117	Verify the /etc/audit/auditd.conf has the disk_full_action and disk_error_action parameters set. Procedure: # grep disk_full_action /etc/audit/auditd.conf # grep disk_error_action /etc/audit/auditd.conf	disk_full_action parameter is found and is not set to “suspend” or “ignore” disk_error_action parameter is found and is not set to "suspend" or "ignore"	
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 []			

Step	Step Description	Expected Results/Comments	P/F
118	Check /etc/audit/auditd.conf for the space_left_action and action_mail_accnt parameters.	the space_left_action or the action_mail_accnt parameters are not set to blanks the space_left_action is set to "syslog" If the space_left_action is set to "exec", the system executes a designated script. the space_left_action parameter is not set to "ignore" or "suspend" the space_left_action parameter is not set to "single" or "halt" the space_left_action is set to "email" and the action_mail_acct parameter is set to the e-mail address of the system administrator The action_mail_acct parameter, if missing, defaults to "root". Note that if the email address of the system administrator is on a remote system "sendmail" must be available.	
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 []			
119	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 []			
120	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 []			
121	# date	Time is set to GMT	

Step	Step Description	Expected Results/Comments	P/F
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.			
122	Check if NTP running: # ps -ef | egrep "xntpd|ntpd" Check if "ntpd -qg" scheduled to run: # grep "ntpd -qg" /var/spool/cron/* # grep "ntpd -qg" /etc/cron.d/* # grep "ntpd -qg" /etc/cron.daily/* # grep "ntpd -qg" /etc/cron.hourly/* # grep "ntpd -qg" /etc/cron.monthly/* # grep "ntpd -qg" /etc/cron.weekly/* If NTP is running or "ntpd -qg" is found: # more /etc/ntp.conf Confirm the timeservers and peers or multicast client (as applicable) are local or authoritative U.S. DoD sources appropriate for the level of classification which the network operates.	a local/authoritative time-server is used	
123	Check the root crontab (crontab -l) and the global crontabs in /etc/crontab, /etc/cron.d/*, or scripts in the /etc/cron.daily directory for the presence of an "ntpd -qg" job.	the "ntpd -qg" command is invoked with at least two external NTP servers listed	
124	Check the NTP daemon configuration for at least two external servers. # grep ^server /etc/ntp.conf | egrep -v '(127.127.1.0|127.127.1.1)'	Two or more servers/external reference clocks (127.127.x.x other than 127.127.1.0 or 127.127.1.1) are listed The NTP server listed is not outside of the enclave	
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 []			

Step	Step Description	Expected Results/Comments	P/F
125	Perform the following to determine the location of audit logs and then check the ownership. Procedure: # grep "^log_file" /etc/audit/auditd.conf|sed s/^[^\/]*//|xargs stat -c %U:%n	all audit log file are owned by root all audit log file are group-owned by root, bin, sys, or system all audit log file has a mode less permissive than 0640 the permissions do not include a '+', the indication the file has an extended ACL	
126	Verify the audit tool executables are owned by root. # ls -l /sbin/auditctl /sbin/auditd /sbin/ausearch /sbin/aureport /sbin/autrace /sbin/audispd Verify the audit tool executables are group-owned by root, bin, sys, or system. Procedure: # ls -lL /sbin/auditctl /sbin/auditd /sbin/ausearch /sbin/aureport /sbin/autrace /sbin/audispd	all listed file are owned by root all listed file are group-owned by root, bin, sys, or system all listed file has a mode less permissive than 0750 the permissions do not include a '+', the indication the file has an extended ACL	
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 []			
127	Review audit storage capacity policy and procedures.	. . . not less than weekly	
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 []			
128	Review non-repudiation policies and procedures		
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.			

Step	Step Description	Expected Results/Comments	P/F
129	Review non-repudiation policies and procedures	. . . 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.	
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 []			
130	Determine if auditing is enabled. # ps -ef |grep auditd	auditd process is found	
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 []			
131	Review Security Assessment And Authorization Policies And Procedures	. . . at least annually if not otherwise defined in formal organizational policy	
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 []			
132	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 []			

Step	Step Description	Expected Results/Comments	P/F
133	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 []			
134	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 []			
135	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	
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;			
136	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	

Step	Step Description	Expected Results/Comments	P/F
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 . . .			
137	Verify the system will not log in accounts with blank passwords. # grep nullok /etc/pam.d/system-auth /etc/pam.d/system-auth-ac	No entry for nullok is found	
138	Check for the existence of the files. # find / -name .rhosts # find / -name .shosts # find / -name hosts.equiv # find / -name shosts.equiv	The files are not found. (If they are, they have been documented and approved by the IAO.)	
139	Check for an enabled "debug" command provided by the SMTP service. Procedure: # telnet localhost 25 debug	the command returns a 500 error code of "command unrecognized" or a 550 error code of "access denied"	
140	# grep server_args /etc/xinetd.d/tftp	the "-s" parameter is specified	
141	Determine if the system is configured to boot from devices other than the system startup media.	No alternative boot devices	
142	Ask the SA if the system uses removable media for the boot loader.	No removable media for the boot loader	
143	Determine if the system uses the GRUB boot loader; # ls -l /boot/grub/grub.conf	grub.conf file exists, if not, the bootloader on the system has been authorized, justified, and documented	
144	Verify that reboot using the CTRL-ALT-DELETE key sequence has been disabled by performing: # grep ctrlaltdel /etc/inittab	the line returned specifies "/usr/bin/logger", or is commented out	

Step	Step Description	Expected Results/Comments	P/F
145	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			
146	Review least functionality policies and procedures	. . . networking protocols IAW IC and DoD Ports, Protocols and Services guidance	
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			
147	Review Information System Component Inventory policies and procedures	. . . continuously	
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 []			
148	Logging should be enabled for those types of file systems not turning on logging by default. Procedure: # mount	FS, VXFS, HFS, XFS, reiserfs, EXT3 and EXT4 all turn logging on by default. The ZFS file system uses other mechanisms to provide for file system consistency. For other file systems types, the root file system should support journaling, if this is the case, the 'nolog' option should not be set.	
149	Verify local filesystems use journaling. # mount | grep '^/dev/' | egrep -v 'type (ext3|ext4|jfs|reiserfs|xfs| iso9660|udf)'	A mount is not listed	
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 []			
150	Check the system for duplicate account names. Example: # pwck -r	No duplicate account names are found	

Step	Step Description	Expected Results/Comments	P/F
151	Perform the following to ensure there are no duplicate UIDs: # cut -d: -f3 /etc/passwd | uniq -d	No duplicate UIDs are found	
152	Perform the following to check for unnecessary privileged accounts: # grep "^shutdown" /etc/passwd # grep "^halt" /etc/passwd # grep "^reboot" /etc/passwd	No unnecessary privileged accounts exist	
153	Determine if an NFS server is running on the system by: # ps -ef |grep nfsd If an NFS server is running, confirm it is not configured with the insecure_locks option by: # exportfs -v	The results should not look like the following; /misc/export speedy.example.com(rw,insecure_locks)	
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 []			
154	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 []			
155	Review identification and authentication for organizational users policies and procedures	. . . uses multifactor authentication for network access to non-privileged accounts	
156	To determine how the SSH daemon's "HostbasedAuthentication" option is set, run the following command: # grep -i HostbasedAuthentication /etc/ssh/sshd_config If no line, a commented line, or a line indicating the value "no" is returned, then the required value is set.	the required value is set	

Step	Step Description	Expected Results/Comments	P/F
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 []			
157	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 []			
158	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			
159	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			
160	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 []			
161	Review device level identification and authentication policies and procedures	. . . all network connected endpoint devices	
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 []			
162	Review device level identification and authentication policies and procedures		
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 []			

Step	Step Description	Expected Results/Comments	P/F
163	Review device level identification and authentication policies and procedures		
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 []			
164	Review device level identification and authentication policies and procedures		
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 []			
165	Review identifier management policies and procedures	A contractor or government employee and citizenship	
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 []			
166	Check the minimum time period between password changes for each user account is 1 day. # cat /etc/shadow | cut -d ':' -f 4 | grep -v 1	No results are returned	
167	Check the system password length setting. Procedure: Check the password minlen option # grep pam_cracklib.so /etc/pam.d/system-auth Confirm the minlen option is set to at least 15 as in the example below: password required pam_cracklib.so minlen=15	A line is found and the minlen is 15 or more	

Step	Step Description	Expected Results/Comments	P/F
168	Verify no valid password hash in /etc/passwd or /etc/shadow begins with a character other than an underscore (_) or dollar sign ($). # cut -d ':' -f2 /etc/passwd # cut -d ':' -f2 /etc/shadow	any valid password hash is present that has an initial underscore (_) or dollar sign ($) character Note: Locked accounts are indicated by a leading exclamation point (!). System accounts, other than "root", may have an asterisk (*) in the password field. On systems utilizing shadow passwords, the password field in /etc/passwd will be a single "x".	
169	Check all password hashes in /etc/passwd or /etc/shadow begin with '5' or '6'. Procedure: # cut -d ':' -f2 /etc/passwd # cut -d ':' -f2 /etc/shadow	All password hashes present begin with '5' or, '6'	
170	Check the ucredit setting. # grep ucredit /etc/pam.d/system-auth	ucredit is set to -1	
171	Check /etc/pam.d/system-auth for lcredit setting. Procedure: Check the password lcredit option # grep pam_cracklib.so /etc/pam.d/system-auth	line is found and the lcredit option is set to -1 line is found and the dcredit option is set to -1 line is found and the ocredit option is set to -1	
172	Check the max days field (the 5th field) of /etc/shadow. # more /etc/shadow	the max days field is not equal to 0 or greater than 60 for any user	
173	Ask the SA if there are any automated processing accounts on the system. If there are automated processing accounts on the system, ask the SA if the passwords for those automated accounts are changed at least once a year or are locked.	SA indicates passwords for automated processing accounts are changed once per year or are locked	

Step	Step Description	Expected Results/Comments	P/F
174	Check /etc/pam.d/system-auth for a pam_cracklib parameter difok. Procedure: # grep difok /etc/pam.d/system-auth Check for system-auth-ac inclusions. # grep -c system-auth-ac /etc/pam.d/* If the system-auth-ac file is included anywhere # more /etc/pam.d/system-auth-ac | grep difok Ensure the passwd command uses the system-auth settings. # grep system-auth /etc/pam.d/passwd	difok is present and has a value of 8 or greater system-auth-ac is included anywhere and difok is present and has a value of 8 or greater a line "password include system-auth" is found, the password checks in system-auth are applied to new passwords	
175	# ls /etc/security/opasswd # grep password /etc/pam.d/system-auth| egrep '(pam_pwhistory.so| pam_unix.so|pam_cracklib.so)' | grep remember Check for system-auth-ac inclusions. # grep -c system-auth-ac /etc/pam.d/* If the system-auth-ac file is included anywhere # more /etc/pam.d/system-auth-ac | grep password | egrep '(pam_pwhistory.so|pam_unix.so| pam_cracklib.so)' | grep remember	/etc/security/opasswd exists the "remember" option in /etc/pam.d/system-auth is 5 or greater in /etc/pam.d/system-auth-ac is referenced by another file and the "remember" option is set to 5 or greater	

Step	Step Description	Expected Results/Comments	P/F
176	Determine if root has logged in over an unencrypted network connection. Examine /etc/syslog.conf to confirm the location to which "authpriv" messages are being sent. # grep authpriv.* /etc/syslog.conf Once the file is determined, perform the following command: # grep password <file> | more Look for any lines that do not have sshd as the associated service.	root has logged in over the network and sshd is running	
177	Verify no password hashes are present in /etc/passwd. # cut -d : -f 2 /etc/passwd | egrep -v '^(x|*)$'	No password hashes are returned	
178	Check the system for the existence of any .netrc files. Procedure: # find / -name .netrc	No .netrc file exists	
179	Determine if default system accounts (such as those for sys, bin, uucp, nuucp, daemon, smtp) have been disabled. # cat /etc/shadow If an account's password field (which is the second field in the /etc/shadow file) is "*", "*LK*", or is prefixed with a '!', the account is locked or disabled.	No unlocked default system accounts	

Step	Step Description	Expected Results/Comments	P/F
180	The telnet service included in the RHEL distribution is part of krb5-workstation. There are two versions of telnetd server provided. The xinetd.d file ekrb5-telnet allows only connections authenticated through kerberos. The xinetd.d krb5-telnet allows normal telnet connections as well as kerberized connections. Both are set to "disable = yes" by default. Ensure that neither is running. Procedure: Check if telnetd is running: # ps -ef |grep telnetd Check if telnetd is enabled on startup: # chkconfig --list|grep telnet	telnet daemon is not running No entry with "on" is found	

Step	Step Description	Expected Results/Comments	P/F
181	Verify LDAP is running on the system. To check to see if the system is an LDAP server, run: # ps -ef | grep ldap Find out which LDAP is used (if not determined via the command above). # rpm -qa | grep ldap If using nssldap: # grep base /etc/ldap.conf Check to see if the base is set to something besides the default of "dc=example,dc=com". If using openldap: # grep suffix /etc/openldap/slapd.conf Check whether the system is an LDAP client: # grep server /etc/ldap.conf # grep server /etc/openldap/ldap.conf Check whether the server option has an address other than the loopback, then check the nsswitch.conf file: # grep ldap /etc/nsswitch.conf Look for the following three lines: passwd: files ldap shadow: files ldap group: files ldap If all three files are not configured to look for an LDAP source, then the system is not using LDAP for authentication. If the system is not using LDAP for authentication, this is not applicable. Check for the "bindpw" option being used in the "/etc/ldap.conf" file. # grep bindpw /etc/ldap.conf	an uncommented "bindpw" option is returned, and a cleartext password is not in the file	

Step	Step Description	Expected Results/Comments	P/F
182	Verify the system-auth settings are being applied. Procedure: Verify the additional pam.d requirements are in use. The file "/etc/pam.d/system-auth-ac" is auto generated by "authconfig". Any manual changes made to it will be lost next time "authconfig" is run. Check to see if the systems default of the symlink "/etc/pam.d/system-auth" pointing to "/etc/pam.d/system-auth-ac" has been changed. # ls -l /etc/pam.d/system-auth If the symlink points to "/etc/pam.d/system-auth-ac", manual changes cannot be protected. This is a finding. # grep system-auth-ac /etc/pam.d/system-auth	The local system-auth file pointed to by "/etc/pam.d/system-auth" must contain "/etc/pam.d/system-auth-ac" for the auth, account, password, and session lines.	
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 []			
183	This system does not utilize PKI-base authentication		
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 []			
184	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 []			
185	Log out of the system	User is logged out	

Step	Step Description	Expected Results/Comments	P/F
186	Log into the system	When entering the password into the system, there should be no feedback (i.e. no asterisks representing the number of characters entered)	
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 []			
187	Verify the algorithm used for password hashing is of the SHA-2 family. # egrep "password .* pam_unix.so" /etc/pam.d/system-auth-ac # egrep "ENCRYPT_METHOD" /etc/login.defs # egrep "crypt_style" /etc/libuser.conf	the hash algorithm is set to sha256 or sha512	
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 []			

Step	Step Description	Expected Results/Comments	P/F
188	Review the System Security Plan	A System Security Plan exists and it: - 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;	
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 []			
189	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 []			
190	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 []			
191	Complete the Discovery Meeting Checklist	The outcomes of the discovery meeting are; - System security categorization, Reference FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004, p. 1 - 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 []			
192	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 []			
193	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 []			
194	Review acquisitions policies and procedures	Included, but not limited to, in the list of artifacts are; - Security Plan (SP) or System Security Authorization Agreement (SSAA) with Attachment 11s - Trusted Facility Manuals (TFM) - Software Version Description Documents (SVDD) - Security Features Users Guides (SFUG) - Initial Equipment Inventory with Hostnames and IP Addresses included - Diagrams/Drawings - 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 []			
195	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 []			
196	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 []			
197	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 []			
198	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 []			
199	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 []			
200	Review security engineering principles		

Step	Step Description	Expected Results/Comments	P/F
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 []			
201	Review external information system services		
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 []			
202	Review external information system services	Chief Information Officer	
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 []			
203	Review developer configuration management		
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 []			
204	Check the root crontab (crontab -l) and the global crontabs in "/etc/crontab", "/etc/cron.*" for the presence of an rpm verification command such as: `rpm -qVa | awk '$2!="c" {print $0}'`	cron job is found	
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 []			

Step	Step Description	Expected Results/Comments	P/F
205	Review developer security testing	. . . the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements	
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 []			
206	Review supply chain protection	Measures in accordance with CNSS Directive 505, Supply Chain Risk Management.	
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 []			
207	Review supply chain protection	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.	
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 []			
208	Review application partitioning policies and procedures	user functionality is limited by group permission assignment	
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 []			
209	Review application partitioning policies and procedures	user must enter privileged (.priv) credentials to access management functions of the system	
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 []			
210	Review information in shared resources		

Step	Step Description	Expected Results/Comments	P/F
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 []			
211	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	
212	Verify the system configured to use TCP syncookies when experiencing a TCP SYN flood. # cat /proc/sys/net/ipv4/tcp_syncookies	the result is "1"	
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 []			
213	Review denial of service protection		
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 []			
214	# svcs network/ipfilter	ipfilter service is listed	
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 []			
215	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 []			
216	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 []			
217	# ipfstat -i	block in log quick on <network interface> from any to any	

Step	Step Description	Expected Results/Comments	P/F
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 []			
218	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 []			
219	Check the firewall rules for a default deny rule. # iptables --list Example of a rule meeting this criteria: REJECT all -- anywhere anywhere reject-with icmp-host-prohibited A rule using DROP is also acceptable. The default rule should be the last rule of a table and match all traffic.	a default deny rule exists	
220			
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 []			
221	Review boundary protection		
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 []			

Step	Step Description	Expected Results/Comments	P/F
222	Review boundary protection scheme policies and procedures	. . . all internal communications traffic, except traffic specifically exempted by the Authorizing Official or organizational policy . . . 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 [] **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 []**			
223	Read system Interface Control Document and interview system administrators	. . . cross domain solutions and controlled interfaces	
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 []			
224	Determine if the system is using a local firewall. # chkconfig --list iptables	the service is "on" in the standard runlevel (ordinarily 3 or 5)	
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 . . .			
225	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 []			
226	Review boundary protection		
Test 110 SC-8 Transmission Integrity: The information system protects the integrity of transmitted information. NSS Defined Value [], AF Defined Value []			
227	Review the system Interface control document (ICD)	Check for use of protocols that ensure integrity of transmissions (i.e. TCP which everyone uses)	
Test 111 SC-9 Transmission Confidentiality: The information system protects the confidentiality of transmitted information. NSS Defined Value [], AF Defined Value []			
228	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 []			
229	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 []			
230	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 []			
231	Review network disconnect policies and procedures	. . . not more than 1 hour	
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.			
232	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 []			
233	Review use of cryptography		
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 []			
234	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 []			
235	Review public access protections		

Step	Step Description	Expected Results/Comments	P/F
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 []			
236	Review collaborative computing devices policies and procedures	Remote activation of centrally managed dedicated VTC Suites located in approved VTC locations	
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 []			
237	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 []			
238	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.			
239	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			
240	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 []			
241	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 []			
242	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. **(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.** **(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.** **(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).** **(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
243	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. (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. (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. (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). (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 []			
244	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 []			
245	Review mobile code	. . . e-mail . . . 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 []			
246	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 []			
247	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 []			
248	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 []			
249	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 []			
250	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 []			
251	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
252	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 []			
253	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 []			
254	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 []			
255	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			
256	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 []			
257	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 []			

Step	Step Description	Expected Results/Comments	P/F
258	Ask the SA if a root kit check tool is run on the system weekly. The only viable process to detect for root kits is to bring the system completely down, boot the system from media that has the root kit scanner, and then scan each of the systems partitions. While it is possible that this could be performed in an automated fashion by an application such as BladeLogic it is more likely that the site/program will have to perform this activity manually to meet the requirement.	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 []			
259	Determine if the /home path is a separate filesystem. # grep "/home " /etc/fstab	result is returned and /home is on a separate filesystem	
260	Determine if the /var path is a separate filesystem. # grep /var /etc/fstab	result is returned and /var is on a separate filesystem	
261	Determine if the /var/log/audit path is a separate filesystem. # grep /var/log/audit /etc/fstab	result is returned and /var/log/audit is on a separate filesystem	
262	Determine if the /tmp path is a separate filesystem. # egrep "[\t]/tmp[\t]" /etc/fstab	result is returned and /tmp is on a separate filesystem	
263	Ask the SA if this is an NMS server. If it is an NMS server, then ask what other applications run on it.	Only network management software and DBMS software used only for the storage and inquiry of NMS data	

Step	Step Description	Expected Results/Comments	P/F
264	If the system is a VM host and acts as a router solely for the benefit of its client systems, then this rule is not applicable. Check to see if the system is a router: # chkconfig --list | grep :on | egrep '(ospf|route|bgp|zebra|quagga)' If the system is running a routing service, it is a router. If it is not, this is not applicable. Check the system for non-routing network services. Procedure: # netstat -a | grep -i listen # ps -ef	No non-routing services, including Web servers, file servers, DNS servers, or applications servers, but excluding management services such as SSH and SNMP, are running on the system	
265	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.	Yes	
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 []			
266	# cd <virus definition folder>		

Step	Step Description	Expected Results/Comments	P/F
267	# ls –la *.dat clean.dat names.dat scan.dat Check for the existence of a cron job to execute a DoD-approved command-line scan tool daily. Other tools may be available but will have to be manually reviewed if they are installed. In addition, the definitions files should not be older than 7 days. Check if DoD-approved command-line scan tool is scheduled to run: # grep [scan tool] /var/spool/cron/* /etc/cron.d/* /etc/cron.daily/* /etc/cron.hourly/* /etc/cron.monthly/* /etc/cron.weekly/*	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 []			
268	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 []			
269	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. IC IRC and AF ISR IRC objectives **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 []** **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 []**			
270	# ps –ef | grep <hbss agent>	The service should be present.	
271	Ask the SA or IAO if a host-based intrusion detection application is loaded on the system. The preferred intrusion detection system is McAfee HBSS available through Cybercom.	HBSS	

Step	Step Description	Expected Results/Comments	P/F
272	Another host-based intrusion detection application, such as SELinux may be used on the system. Procedure: Examine the system to see if the Host Intrusion Prevention System (HIPS) is installed #rpm -qa | grep MFEhiplsm If the MFEhiplsm package is installed, HBSS is being used on the system. If another host-based intrusion detection system is loaded on the system # find / -name <daemon name> Where <daemon name> is the name of the primary application daemon to determine if the application is loaded on the system. Determine if the application is active on the system. Procedure: # ps -ef | grep <daemon name>	A host-based intrusion detection system is installed on the system	
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 []			
273	Review Information System Monitoring		
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.			

Step	Step Description	Expected Results/Comments	P/F
274	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 []			
275	Check permissions on IPfilter settings		
276	Check permissions on antivirus settings		
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.			
277	Review information system monitoring policies and procedures	(1) . . . incident response personnel (2) . . . the least disruptive action to terminate suspicious events as determined appropriate for the individual system.	
278	For each security tool on the system, determine if the tool is configured to notify the IAO and SA of any detected security problem.	such notifications are configured	
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 []			
279	Interview (DPOC) network administrators about outbound communications monitoring.	The DPOC 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 []			
280	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
281	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 2 . . . at least every 90 days			
282	Check virus scanning and review security functionality verification policies and procedures	(1). . . upon system startup and/or restart (2). . . at least every 90 days (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 []			
283	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 []			
284	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 []			

Step	Step Description	Expected Results/Comments	P/F
285	If the system uses sendmail examine the configuration files. Determine if sendmail only binds to loopback addresses by examining the "DaemonPortOptions" configuration options. Procedure: # grep -i "O DaemonPortOptions" /etc/mail/sendmail.cf determine if sendmail is configured to allow open relay operation. Procedure: # grep -i promiscuous_relay /etc/mail/sendmail.mc If the system uses Postfix, locate the main.cf file. Procedure: # find / -name main.cf Determine if Postfix only binds to loopback addresses by examining the "inet_interfaces" line. Procedure: # grep inet_interfaces </path/to/main.cf> Determine if Postfix is configured to restrict clients permitted to relay mail by examining the "smtpd_client_restrictions" line. Procedure: # grep smtpd_client_restrictions </path/to/main.cf>	uncommented DaemonPortOptions lines, and all such lines specify system loopback addresses No promiscuous relay feature "inet_interfaces" is set to "loopback-only" or contains only loopback addresses such as 127.0.0.1 and [::1], Postfix is not listening on external network interfaces the "smtpd_client_restrictions" line is not missing, or/and contains "reject" the line contains "reject" before "permit"	
Test 160 SI-8 (1) Spam Protection: The organization centrally manages spam protection mechanisms. NSS Defined Value [], AF Defined Value []			
286	(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 []			
287	(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 []			
288	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.	
289	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 []			
290	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			
291	Check the mode of log files. Procedure: # find /var/log /var/log/syslog /var/adm -type f -perm -640 \! -perm 640 Verify system log files have no extended ACLs. Procedure: # ls -lL /var/log	With the exception of /var/log/wtmp, /var/log/Xorg.0.log, and /var/log/gdm/:0.log, the log files have modes less permissive than 0640 If the permissions include a '+', the file has an extended ACL. If an extended ACL exists, verify with the SA if the ACL is required to support authorized software and provides the minimum necessary permissions.	
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 []			
292	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	

Step	Step Description	Expected Results/Comments	P/F
Notes:			

4.2 Reporting

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