Revised SITE1A CyberSecurity Compliance Self-Test Plan, Linux

March 2025

STP Revised Steps

To be run on the utility node

Step	Step Description	Step Command	Expected Results	P/F
Test 1 AC-2 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. Test: True (test that there are no accounts with UID 0 except root in the /etc/passwd file	$ 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. The lP and ftp users are now removed	
2	Check /etc/pam.d/su uses pam_wheel.	$ grep pam_wheel /etc/pam.d/su	**auth [success=1 default=ignore] pam_wheel.so trust** **auth require pam_wheel.so user_uid group=wheel**	
3	check to make sure /etc/passwd is owned by root	$ ls -l /etc/passwd	**-rw-r--r--. 1 root root 2184 Mar 19 20:56 /etc/passwd**	
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 []				
4	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) No Temporary, guest, anonymous, application, or special accounts created. b. Establishing conditions for group membership Group accounts have to meet certain conditions, only if the accounts are required for mission work. c. Identifying authorized users of the information system and specifying access privileges All authorized users acquire specific privileges/access depending on need-to-know, duties and job titles. This is determined	

			by the ISSM / ISSO and Contract manager. d. Requiring appropriate approvals for requests to establish accounts All accounts have to be approved by the ISSO, ISSM, and their manager prior to establishing an account, the user needs to review the user agreement documentation and acknowledge (signing) the documentation prior to them receiving their account/s e. Establishing, activating, modifying, disabling, and removing accounts The contract engineer/system administrator establishes, activates, modifies, disables, and manages accounts (remove, modify, lock). Their responsibilities include informing the contract manager, ISSO, ISSM, and ISSE, keeping / updating the user documentation worksheet, and informing the security group if user/s require debriefing.	
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 []				
5	Check the date in the "last" log to verify it is within the last 90 days or the maximum number 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	$ cut -d: -f1 /etc/passwd | xargs -n 1 sudo /bin/passwd -S	No inactive account is not disable 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. No local accounts or temporary accounts allowed. Should get result as follows if there is an output **# root LK 2024-10-04 0 99999 7 -1 (Password locked.)**	

	must be done in the BASH Shell.			
6	verify the "INACTIVE" setting, run the following command: /etc/default/useradd	sudo cat /etc/default/useradd | grep INACTIVE	indicate the "INACTIVE" configuration option is set to an appropriate integer as shown in the example below: **INACTIVE=35**	
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 []				
7	Determine if execution of the useradd and groupadd executable are audited. Determine if /etc/passwd, /etc/shadow, /etc/group, and /etc/gshadow are audited for appending. Determine if execution of the passwd executable is audited. Determine if execution of the userdel and groupdel executable are audited.	# sudo auditctl -l | egrep '(useradd | groupadd)' # sudo auditctl -l | egrep '(/etc/passwd | /etc/shadow | /etc/group | /etc/gshadow)' # sudo auditctl -l | grep /usr/bin/passwd	- Returns nothing as functions not audited. - Returns **-w /etc/passwd -p wa -k identity** **-w /etc/group -p wa -k identity** **-w /etc/gshadow -p wa -k identity** **-w /etc/shadow -p wa -k identity** **-w /etc/passwd -p wa -k audit_account_changes** **-w /etc/group -p wa -k audit_account_changes** **-w /etc/gshadow -p wa -k audit_account_changes** **-w /etc/shadow -p wa -k audit_account_changes** Returns: **-a always,exit -S all -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=-1 -F key=privileged-passwd** **-a always,exit -S all -F path=/usr/bin/passwd -F perm=x -F auid>=1000 -F auid!=-1 -F key=setuid/setgid** **-w /usr/bin/passwd -p x -k privileged-passwd**	
Test 9 AC-2(5) Account Management: Inactivity Logout 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 []				
8	check logout gnome screensaver	$ rpm -qa | grep -i gnome	no returns as gnome is not installed on the servers	
Test 6 AC-2 (10) Account Management: The Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers.				
9	Review account		Procedures should include role-	

	establishment and management processes and interview account managers		based access schemes and a mechanism for tracking role assignment.	
Test 6 AC-2 (10) Account Management: The Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers.				
10	On systems with a UEFI or system controller, verify a supervisor or administrator password is set. Check the "/boot/efi/EFI/ redhat/grub.conf" or "/boot/efi/redhat/ menu.1st" files.	Password is required. The correct file should be grub.cfg The new command will be: **sudo cat /boot/efi/EFI/redhat/grub.cfg**	You will see the contents of grub.cfg It begins with **#** **# DO NOT EDIT THIS FILE** **#** **# It is automatically generated by grub2-mkconfig using templates** **# from /etc/grub.d and settings from /etc/default/grub** **#** And ends with **fi** **### END /etc/grub.d/41_custom ###**	
Test 7 AC-3 Account Management: The information system enforces responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers]				
11	On systems with a UEFI or system controller, verify a supervisor or administrator password is set.	sudo cat /etc/grub.d/01_users | grep password	**password_pbkdf2 root \$ {GRUB2_PASSWORD}**	
12	Check GRUB for password configuration.	sudo cat /boot/efi/EFI/redhat/grub.cfg | grep -i password	if [-n "${**GRUB2_PASSWORD}"]; **then** **password_pbkdf2 root ${GRUB2_PASSWORD}**	
13	Check contents of grub.conf	Cat /etc/grub.conf	**cat: /etc/grub.conf: No such file or directory** is returned as this is UEFI as shown in previous commands	
14	Oracle Enterprise Linux operating systems versions 8.10 or new with a basic input/output system (BIOS/UFI) must require authentication upon booting. Hitting F	Log into BIOS. If you want to validate length of password Refer to email that was sent 11/19/2024		

	key on boot requires BIOS/UFI password.			
Test 7 AC-3(2) Access Enforcement: The information system enforces enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. NSS Defined Value [], AF Defined Value []				
15	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. This includes all system, network administrators, or organizational personnel.	
16	Dual authorization mechanisms implementing access control policy • AC-3(2)(1) The organization defines privileged commands and/or other actions for which dual authorization is to be enforced;		Dual authorization is not being implemented	
Test 7 AC-3(3) Access Enforcement: The information system enforces enforcement responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers []				
17	• AC-3(3)[1] the organization defines mandatory access control policies to be enforced over all subjects and objects; • AC-3(3)[2] the organization defines subjects over which organization-defined mandatory access control policies are to be enforced;			

	• AC-3(3)[3] the organization defines objects over which organization-defined mandatory access control policies are to be enforced; • AC-3(3)[4] the organization defines subjects that may explicitly be granted privileges such that they are not limited by the constraints specified elsewhere within this control; • AC-3(3)[5] the information system enforces organization-defined mandatory access control policies over all subjects and objects where the policy specifies that: • AC-3(3)[6] the policy is uniformly enforced across all subjects and objects within the boundary of the information system;			
Test 7 AC-3 (4) Access Enforcement: The information system enforces responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers [], AF Defined Value []				
18	• AC-3(4)[2] Responsibilities; system/network administrators; organizational		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility	

	personnel with information security responsibilities; system developers • AC-3(4)[2]a Pass the information to any other subjects or objects; • AC-3(4)[2]b Grant its privileges to other subjects; • AC-3(4)[2]c Change security attributes on: • AC-3(4)[2]d Choose the security attributes to be associated with newly created or revised objects; or • AC-3(4)[2]e Change the rules governing access control.		and document the value(s) within the body-of-evidence. The ISSM/ISSO work with the OEM to assure all users are given access according to their job titles, need to know, and responsibilities. The security team assures that all accounts are being documented, and as soon as a person leaves, gets fired, promoted, or responsibilities change, the account is locked and removed. The change of responsibilities needs to be updated, and the security team informed.	
19	Verify only users has read, write execute permissions	sudo cat /etc/login.defs | grep -i umask	**UMASK 077**	
The information system enforces responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers [], AF Defined Value []				
20	• AC-3(5)[1] The organization defines security-relevant information to which the information system prevents access except during secure, non-operable system states; and • AC-3(5)[2] The information system prevents access to organization-defined security-		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and documenting the value(s) within the body-of-evidence. The ISSM/ISSO work with the OEM to assure all security-relevant information and assure that it prevents user access during a non-operable system state.	

	relevant information except during secure, non-operable system states.			
Test 3 AC-3 (7) Access Enforcement: Role-Based Access Control Responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers, AF Defined Value []				
21	• **AC-3(7)[1]** The organization defines roles to control information system access. • **AC-3(7)[2]** The organization defines users authorized to assume the organization-defined roles. • **AC-3(7)[3]** The information system controls access based on organization-defined roles and users authorized to assume such roles. • **AC-3(7)[4]** The information system enforces a role-based access control policy over defined roles.		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and documenting the value(s) within the body-of-evidence. This includes communication with the OEM/Engineering team. The roles and security privileges depend on the user's responsibilities, need to know, and contract. TFM User Groups and Access Rights User rights and access are determined based on role and job function and enforced through group assignments using a least privilege practice. • The VIP-C enforces replay-resistant authentication mechanisms using Kerberos (Windows only). • In addition to normal user accounts, the VIP-C system restricts additional users/groups to a subset of all available functionality. • Group accounts are prohibited for shared login use. Service accounts are created for non-interactive login that is common with many applications requiring authentication to function properly. • Dual authorization is required for running any privileged command. Users must escalate using the OS built-in tools (e.g., sudo) to perform privileged operations. • No multifactor authorization mechanisms are currently implemented within the VIP-C.	
Test 8 AC-3 (8) Access Enforcement: The information system enforces responsibilities; system/network administrators; organizational personnel with information security				

responsibilities; system developers.				
22	AC-3(8)[1] The organization defines rules governing the timing of revocations of access authorizations; and AC-3(8)[2] The information system enforces the revocation of access authorizations resulting from changes to the security attributes of subjects and objects based on organization-defined rules governing the timing of revocations of access authorizations.		CNSS Revocation of Access Administrators have the capability of revoking user access or group membership in accordance with site policy (SOP). CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and documenting the value(s) within the body-of-evidence. The security team follows Air Force-defined rules governing the timing of revocations of access authorization. The ISSO/ISSM informs the OEM/Engineers of any revocation of access resulting from changes to attributes of subjects/objects.	
Test 8 AC-3(9) Access Enforcement: The information system enforces responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers. NSS Defined Value [], AF Defined Value []				
23	AC-3(9) [1] The organization defines the information system or system component authorized to receive information released outside of the established system boundary of the information system releasing such information; AC-3(9) [2] The organization defines security safeguards to be provided by organization-defined information system or system component receiving information released from an information system outside of the established		TFM Boundary protection within the scope of its own infrastructure and in conformance with site requirements and DoD policy. Boundary protection outside the VIP-C network is considered a site responsibility. In terms of how the VIP-C addresses boundary protection, the following key points should be noted: -Implements firewalls and network separation to enforce security policies on interconnected systems. Firewalls are all software-based and reside on all hosts (Windows, Linux, Solaris, and ESXi). They are configured to only allow specific port access into the host based on services it offers. An implicit deny rule is set up to drop traffic destined for foreign ports. - No publicly accessible information. All systems within the VIP-C network are only accessible when successfully authenticated	

	system boundary; AC-3(9) [3] The organization defines security safeguards to be used to validate the appropriateness of the information designated for release; AC-3(9) [4] The information system does not release information outside of the established system boundary unless:		using known credentials. Public access (shared accounts, anonymous accounts, etc.) is disallowed. - Does not release information outside its boundary unless externally permitted through the change management/approval process. Part of that process includes approval of ports, protocols, and services (PPS) to allow specific traffic to flow between defined endpoints. - Only allows incoming communications within the same subnet or from other known/trusted subnets. SCAP The Oracle Enterprise Linux operating system must be configured so that all networked systems have SSH installed. Test type: Automatic Result: Pass Version: OEL-07-040300 ISSO/ISSM defines security safeguards (information/components) which are authorized for systems outside of established system boundary.	
Test 8 AC-3 (10) Access Enforcement: The information system enforces responsibilities; system/network administrators; organizational personnel with information security responsibilities [ ], AF Defined Value [ ]				
24	AC-3(10) [1] defines conditions under which to employ an audited override of automated access control mechanisms; and AC-3(10) [2] employs an audited override of automated access control mechanisms under organization-defined conditions		Audited Activities The following key points are relevant to audited activities: Each operating system has a built-in auditing capability that is maximized to its full potential (within the scope of requirements) to capture specific user activities. The basis for designating auditing activities is derived from NIST 800-53 in conjunction with DoD-recommended values and site-specific SOP requirements (SOP #3 Table 7.0). • CheckMate leverages LDAP to ensure each audited activity produced by the OS is valid and provides sufficient	

			traceability. • Auditing rules are maintained through the Puppet configuration management system for Linux hosts. Management of other operating systems. • Custodians and site ISSOs are responsible for ensuring that the audit data produced meets site security requirements and that only security-relevant audit data is produced to provide targeted results. This validation is performed whenever a change of infrastructure components warrants re-evaluation. The site ISSOs are responsible for reviewing audit data delivered to the central log collection per their SOP. VIP-C custodians will perform internal reviews as necessary when site ISSOs are unavailable and/or when reviews are triggered by a particular event. CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and documenting the value(s) within the body-of-evidence.	
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 []				
25	Verify the system does not accept source-routed IPv4 packets.	sudo cat /proc/sys/net/ipv4/conf/all/accept_source_route sudo cat /proc/sys/net/ipv4/conf/default/accept_source_route	should return the following for both commands **0**	
26	Verify the system does not respond to ICMP TIMESTAMP_REQUESTs	sudo cat /etc/sysconfig/iptables | grep "timestamp"	This should return no entries as there is no "timestamp-reply" or "timestamp_request"	
27	Verify the system does not respond to ICMP ECHO REQUESTs set to broadcast	sudo cat /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts	Result is **1**	

	addresses.			
28	Verify the system does not respond to ICMP TIMESTAMP REQUESTs set to broadcast addresses.	sudo cat /proc/sys/net/ipv4/icmp_ignore_bogus_error_responses	Result is **1**	
29	Verify the system does not use proxy ARP.	sudo cat /proc/sys/net/ipv4/conf/all/proxy_arp sudo cat /proc/sys/net/ipv4/conf/default/proxy_arp	Results for both commands should be **0**	
30	Verify the system does not accept IPv4 ICMP redirect messages.	sudo cat /proc/sys/net/ipv4/conf/all/accept_redirects sudo cat /proc/sys/net/ipv4/conf/default/accept_redirects	Results for both commands should be **0**	
31	Verify the system does not send IPv4 ICMP redirect messages.	sudo cat /proc/sys/net/ipv4/conf/all/send_redirects sudo cat /proc/sys/net/ipv4/conf/default/send_redirects	Results for both commands should be **0**	
32	Verify the system is not configured for bridging.	sudo ls /proc/sys/net/	You should not see a folder for bridge only the following: **core ipv4 ipv6 mptcp netfilter nf_conntrack_max unix**	
33	Verify the Bluetooth protocol handler is prevented from dynamic loading.	sudo cat /etc/modprobe.d/modprobe.conf	Result should be empty as there are no dynamic loaders configured.	
34	Verify finger is not present	rpm -qa | grep -i finger	Nothing is returned as finger is not installed	
35	Verify the IPv6 protocol handler is prevented from dynamic loading.	sudo cat /etc/modprobe.d/modprobe.conf	Result should be empty as there are no dynamic loaders configured.	
36	Check the system for any active ipv6to4 tunnels without specific remote addresses.	ip tun list | grep "remote any" | grep "ipv6/ip"	No results returned as no tunnels should be running	
37	Verify the Miredo service is not	rpm -qa | grep -i miredo	No results should be returned as service is not installed	

	running.			
38	Verify the system is configured to ignore IPv6 ICMP redirect messages.	cat /proc/sys/net/ipv6/conf/all/accept_redirects	Returns **0** as it is not enabled	
39	Determine if the system is configured to forward IPv6 source-routed packets.	egrep "net.ipv6.conf.*forwarding" /etc/sysctl.conf	Returns the following as it is not enabled **net.ipv6.conf.all.forwarding = 0**	
Test 10 AC-4(1) Information Flow Enforcement | Object Security Attributes: System/network administrators; organizational personnel with information security responsibilities; system developers [], AF Defined Value []				
40	**AC-4(1)[1]** the organization defines information flow control policies as a basis for flow control **decisions;** **AC-4(1)[2]** the organization defines security attributes to be associated with information, source, and destination objects **AC-4(1)[3]** the organization defines the following objects to be associated with organization-defined security attributes **AC-4(1)[4]** the information system uses organization-defined security attributes associated with organization-defined information, source, and destination objects to enforce organization-defined information flow control policies as a basis for flow control decisions		CNSS Object Security Attributes Information Flow ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence...Not appropriate to define at the AF IC level; the ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence...Not appropriate to define at the AF IC level; the ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence AC-4(1) The information systems uses Air Forces associated with DOD to enforce all basis for flow control decisions.	
Test 10 AC-4(2) Information Flow Enforcement: Processing domains System/network administrators; organizational personnel with information security				

responsibilities. NSS Defined Value [], AF Defined Value []				
41	AC-4(2)[1] the organization defines information flow control policies as a basis for flow control decisions; and AC-4(2)[2] the information system uses protected processing domains to enforce organization-defined information flow control policies as a basis for flow control decisions.		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence All systems have been assign to a Domain, information flows or sharing are controlled based on allowed information accesses allowing signaling / communications among other domains or systems. The information system uses protected processing domain enforcement as a basis for flow control decisions.	
Test 10 AC-4(3) Information Flow Enforcement: Dynamic Information Flow Control System/network administrators; organizational personnel with information security responsibilities; system developers. NSS Defined Value [], AF Defined Value []				
42	AC-4(3)[1] the organization defines policies to enforce dynamic information flow control; and AC-4(3)[2] the information system enforces dynamic information flow control based on organization-defined policies		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. The ISSO / ISSM will work with the OEM/Engineering team to assure that any anomalies or adverse events are being reported, fixed and documented. Dynamic Information Flow Control Organizational policies regarding dynamic information flow control are being implemented throughout the network infrastructure. These information flow controls are modified or implemented depend on changing conditions or mission operational considerations. Dynamic Information Flow Control are also altered due to changes in the immediacy of mission’s needs, government requirements or potential harmful or adverse events.	
Test 10 AC-4(4) Information Flow Enforcement: Content Check Encrypted Information System/network administrators; organizational personnel with information security responsibilities; system developers. NSS Defined Value [], AF Defined Value []				
43	AC-4(4)[1] the organization		CNSS Decrypting the information;	

	defines a procedure or method to be employed to prevent encrypted information from bypassing content-checking mechanisms; AC-4(4)[2] the information system prevents encrypted information from bypassing content-checking mechanisms by doing one or more of the following: To encrypt a file, complete the following: 1. Open a terminal window to a Linux system. 2. At the command prompt, execute the following command: openssl aes-256-cbc -md sha256 -salt -in <plaintext filename> -out <ciphertext filename> The file <plaintext file> will be encrypted and stored in <ciphertext file>. To decrypt a file, complete the following: 1. Open a terminal window to a Linux system. 2. At the command prompt, execute the following command: openssl aes-256-cbc -md sha256 -d -salt -in <ciphertext filename> -out <plaintext filename> The file <ciphertext file> will be decrypted and stored in <plaintext file>.		blocking the flow of the encrypted information; terminating communications sessions attempting to pass encrypted information; and/or... Not appropriate to define at the AF IC level; the ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. TFM Encrypting a file prevents the contents of that file from being read or altered by unauthorized users. The system supports password-based encryption with an AES 256-bit cipher. These procedures may be used to encrypt data that will be stored on the system or copied to external media such as an LTO tape or DVD/Blu-ray disk. The Information system prevents encrypted information from bypassing content checking mechanisms. The network infrastructure (servers, Domain, switches, routers, and firewalls) prevents encrypted information from bypassing content-checking mechanism.	
Test 10 AC-4(5) INFORMATION FLOW ENFORCEMENT | EMBEDDED DATA TYPES **System/network administrators; organizational personnel with information security**				

responsibilities; system developers[], AF Defined Value []				
44	**AC-4(5)[1]** the organization defines limitations to be enforced on embedding data types within other data types; and **AC-4(5)[2]** the information system enforces organization-defined limitations on embedding data types within other data types.		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. Security Team / OEM limit the types of embedded data being passed via the network/systems. Embedding includes any inserting references or descriptive information into a media file and compressed or archived data that may include multiple embedded data types.	
Test 10 AC-4(6) INFORMATION FLOW ENFORCEMENT | METADATA System/network administrators; organizational personnel with information security responsibilities; system developers AF Defined Value []				
45	AC-4(6)[1] the organization defines metadata to be used as a means of enforcing information flow control; and AC-4(6)[2] the information system enforces information flow control based on organization-defined metadata.		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. The ISSO/ISSM work with the OEM / Engineers to ensure sufficiently strong binding techniques with appropriate levels of assurance. This includes the following types of metadata: Structural, or descriptive, enforcing allowed information flows based on metadata enables simpler more effective flow controls.	
Test 10 AC-4(7) INFORMATION FLOW ENFORCEMENT | ONE WAY FLOW MECHANISM System/network administrators; organizational personnel with information security responsibilities; system developers; system developers; system developers AF Defined Value []				
46	AC-4(7)[1] the organization defines one-way information flows to be enforced by the information system; and AC-4(7)[2] the information system enforces organization-defined one-way information		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence One way transfer is being implemented on some systems, downgrading of information is not allow on any of the systems.	

	flows using hardware mechanisms			
Test 10 AC-4(8) Information Flow Enforcement: Security Policy Filter System/network administrators; organizational personnel with information security responsibilities; system developers NSS Defined Value [], AF Defined Value []				
47	**AC-4(8)[1]** the organization defines security policy filters to be used as a basis for enforcing flow control decisions; **AC-4(8)[2]** the organization defines information flows for which flow control decisions are to be applied and enforced; and **AC-4(8)[3]** the information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions for organization-defined information flows.		CNSS ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. Not appropriate to define at the AF IC level; the ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. The ISSO/ISSM defined a security policy filters (SPLUNK, Audit files) which can address data structures and content. Example, security policy filters for data structures can check for maximum file lengths, maximum field size and data/file types. It can also check for specific words (dirty/clean) enumerated values or data value ranges and hidden content.	
Test 10 AC-4(9) Information Flow Enforcement: Human Reviews System/network administrators; organizational personnel with information security responsibilities; organizational personnel with information flow enforcement responsibilities; system developers. NSS Defined Value [], AF Defined Value []				
48	**AC-4(9)1** the organization defines information flows requiring the use of human reviews; **AC-4(9)2** the organization defines conditions under which the use of human reviews for organization-defined information flows is to be enforced; and **AC-4(9)3** the information		ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence, they define security policy filters for all situations where automated flow controls decisions are possible. This is accomplish by using several tools (Splunk, system audits, Nessus, etc.) to monitor and audit information/ traffic. Human reviews may also be employed as deemed necessary by security team.	

	system enforces the use of human reviews for organization-defined information flows under organization-defined conditions.			
Test 10 AC-4(10) INFORMATION FLOW ENFORCEMENT: ENABLE / DISABLE SECURITY POLICY FILTERS **Organizational personnel with responsibilities for enabling/disabling security policy filters; system/network administrators; organizational personnel with information security responsibilities; system developers. NSS Defined Value [], AF Defined Value []**				
49	**AC-4(10)1** the organization defines security policy filters that privileged administrators have the capability to enable/disable **AC-4(10)2** the organization-defined conditions under which privileged administrators have the capability to enable/disable organization-defined security policy filters; and **AC-4(10)3** the information system provides the capability for privileged administrators to enable/disable organization-defined security policy filters under organization-defined conditions		CNSS Security policy filters approved by the AF IC AO… to support operational / mission requirements. Security Authorization administration enabling / disabling of security policy filters falls on the system engineer / administrator. The security team works with their OEM partners to assure the filters and auditing configuration are in par with the Air Force recommendations. Disabling or enabling of filters requires Security concurrence prior to the disabling or enabling of these policies.	
Test 11 AC-4(11) INFORMATION FLOW | CONFIGURATION OF SECURITY POLICY FILTERS **Organizational personnel with responsibilities for configuring security policy filters; system/network administrators; organizational personnel with information security responsibilities; system developers**				
50	**AC-4(11)1** the organization defines security policy filters that privileged administrators have		CNSS The ISSO/ISSM is responsible for determining the value in collaboration with the appropriate office of primary responsibility and document the values within the	

	the capability to configure to support different security policies; and **AC-4(11)2** the information system provides the capability for privileged administrators to configure organization-defined security policy filters to support different security policies.		body of evidence. To reflect changes in security policies the administrator / engineer needs to inform the ISSO / ISSM of any changes to any security policies as they are being tracked by the security team via a variation of tools (Splunk, Nessus, ACAS, EPO and audit files).	
Test 10 AC-4(12) Information Flow Enforcement: Data Type Identifiers System/network administrators; organizational personnel with information security responsibilities; system developers. NSS Defined Value [], AF Defined Value []				
51	**AC-4(12)1** the organization defines data type identifiers to be used, when transferring information between different security domains, to validate data essential for information flow decisions; and **AC-4(12)2** the information system, when transferring information between different security domains, uses organization-defined data type identifiers to validate data essential for information flow decisions.		CNSS The ISSO/ISSM is responsible for determining the value in collaboration with the appropriate office of primary responsibility and document the values within the body of evidence. Data type identifiers include, for example, filenames, file types, file signatures/tokens, and multiple internal file signatures/tokens. Information systems may allow transfer of data only if compliant with data type format specifications. The information system, when transferring information between different security domains, uses to validate data essential for information flow decisions. The access control policy defines the scope of responsibility relative to management of users and roles in compliance. The process in which users are granted access to the system conforms to NIST 800-53 (ICD 503) control policies. User accounts and roles are granted by an authorizing agent (e.g., IS owner, AO, or ISSO) after reviewing the scope of responsibilities and requirements for a particular user. Each user is briefed for access to the systems and any information	

			stored or accessed on the system. Users possess the need-to-know for any information to which they have access, have valid access requirements, and are security briefed and technically trained. Regulations governing the operational environment the organization determine the classification requirements for the user. In a non-operational situation, a minimum of a Secret clearance and a need-to-know validated by a responsible point of contact at site is required to access sensitive data generated by the systems.	
Test 10 AC-6 Least Privilege System/network administrators; Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators. NSS Defined Value [], AF Defined Value []				
52	Check the permissions on the files or scripts executed from system startup scripts to see if they are world-writable.	ls -l /etc/init.d/* | tr '\011' ' ' | tr -s ' ' | cut -f 9,9 | grep -v cma	**-rw-r--r--. 1 root root 18434 Aug 10 2022 /etc/init.d/functions -rwxr-xr-x. 1 root root 9152 Apr 18 2023 /etc/init.d/iptables -rwxr--r--. 1 root root 1190 Apr 18 2023 /etc/init.d/iptables-retry -rwxr-xr-x. 1 root root 23982 Dec 7 2023 /etc/init.d/ma -rwxr-xr-x. 1 root root 2633 Apr 20 2021 /etc/init.d/metricbeat -r-xr-x---. 1 root postgres 497 Apr 25 2023 /etc/init.d/nfgraph -rw-r--r--. 1 root root 3599 Feb 20 2024 /etc/init.d/opensearch -rw-r--r--. 1 root root 4174 Feb 20 2024 /etc/init.d/opensearch-dashboards -rw-r--r--. 1 root root 1161 May 23 2024 /etc/init.d/README -rwxr-xr-x. 1 root root 5387 Apr 20 2022 /etc/init.d/snortd -rwxr-xr-x. 1 root root 10768 Feb 5 22:29 /etc/init.d/vmware -rwxr-xr-x. 1 root root 2872 Feb 5 22:28 /etc/init.d/vmware-USBArbitrator -rwxr-xr-x. 1 root wazuh 1175 Jun 3 2022 /etc/init.d/wazuh-manager**	
53	If /etc/shells exists, check the group ownership of	ls /etc/shells _____	Returns **/etc/shells**/	

	each shell referenced.	cat /etc/shells | xargs ls -l	_____ returns **rwxr-xr-x. 1 root root 1150576 May-22 2024 /bin/bash** **lrwxrwxrwx. 1 root root 4 May 22 2024 /bin/sh -> bash** **rwxr-xr-x. 1 root root 12152 Apr-10 2024 /sbin/nologin** **rwxr-xr-x. 1 root root 1150576 May-22 2024 /usr/bin/bash** **lrwxrwxrwx. 1 root root 4 May 22 2024 /usr/bin/sh -> bash** **rwxr-xr-x. 1 root root 12152 Apr-10 2024 /usr/sbin/nologin**	
54	Verify firefox is not installed.	rpm -qa | grep -i firefox	Command returns no results as firefox is not installed on the system	
55	Verify the ownership of files referenced within the send mail aliases file.	cat /etc/aliases	- Will display list of all file contents mailer-daemon: postmaster postmaster: root bin: root daemon: root adm: root lp: root sync: root shutdown: root halt: root mail: root news: root uucp: root operator: root games: root gopher: root ftp: root nobody: root radiusd: root nut: root dbus: root vcsa: root canna: root wnn: root rpm: root nscd: root pcap: root apache: root webalizer: root dovecot: root fax: root quagga: root radvd: root pvm: root amanda: root privoxy: root ident: root	

			named: root xfs: root gdm: root mailnull: root postgres: root sshd: root smmsp: root postfix: root netdump: root ldap: root squid: root ntp: root mysql: root desktop: root rpcuser: root rpc: root nfsnobody: root ingres: root system: root toor: root manager: root dumper: root phen: csa@localhost	
56	Check the shell for the anonymous FTP account.	cat /etc/passwd | grep -i ftp	Returns nothing as there is no ftp user	
57	Check the mode of the TFTP daemon.	ls -l /etc/xinetd.d	Returns total 0 as tftp daemon not running or installed	
58	Check if gnome is installed	$ rpm -qa | grep gnome	nothing returned as gnome is not installed	
59	Perform the following to check for unnecessary privileged accounts.	cat /etc/passwd | grep -E 'shutdown|halt|reboot'	nothing is returned as the accounts do not exist	
60	Determine if an NFS server is running on the system.	ps -ax | grep nfsd | grep -v grep	nothing is returned as nfs is not running on the system	
61	Verify the /etc/passwd file is owned by root.	ls -l /etc/passwd	returns **-rw-r--r--. 1 root root 2184 Mar 19 20:56 /etc/passwd**	
62	Verify the	ls -l /etc/group	Returns	

	/etc/group file is owned by root.		**-rw-r--r--. 1 root root 1088 Mar 19 20:56 /etc/group**	
63	Verify the /etc/shadow file is owned by root.	ls -l /etc/shadow	Returns **----------. 1 root root 1296 Mar 22 19:56 /etc/shadow**	
64	Use pwck to verify home directory assignments are present.	$ sudo pwck	Returns **user 'rngd': directory '/var/lib/rngd' does not exist** **user 'pesign': directory '/run/pesign' does not exist** **Segmentation fault** rngd is used to inject random items and pesign is the package signing utility. They will show up but are not users thus casing a seg fault when running the command. This is normal behavior	
65	Check the /etc/group file for password hashes	cut -d: -f2 /etc/group | egrep -v '^(x|!)$'	Nothing is returned as there are no password hashes stored in the file.	
66	Check the home directory mode of each user in /etc/passwd and verify there are no extended ACL's.	$ ls -lar /home	All of the home directories are listed. Created users will have 750 while service accounts will have 755. None of the users will have a '+'	
67	Check the user/group ownership of each user home directory listed in the /etc/passwd file. Output will contain users with no home directory	cat /etc/passwd | cut -d: -f1,6 | while IFS=: read -r user homedir; do [-L "$homedir"] && continue; echo -n "$user: "; ls -ld "$homedir" 2>/dev/null || echo "Home directory not found"; done	The following is reported. The users rngd and pesign do not have home directories: **root: dr-xr-x---. 18 root root 4096 Mar 22 07:07 /root** **adm: drwxr-xr-x. 2 root root 4096 Oct 9 2021 /var/adm** **mail: drwxrwxr-x+ 2 root mail 4096 Mar 22 20:15 /var/spool/mail** **operator: dr-xr-x---. 18 root root 4096 Mar 22 07:07 /root** **nobody: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 /** **dbus: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 /** **systemd-coredump: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 /** **systemd-resolve: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 /** **polkitd: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 /**	

			postfix: drwxr-xr-x+ 16 root root 4096 Oct 14 2023 /var/spool/postfix chrony: drwxr-x---. 2 chrony chrony 4096 Feb 24 20:13 /var/lib/chrony sssd: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 / sshd: drwx--x--x. 3 root root 4096 Aug 14 2024 /var/empty/sshd rngd: Home directory not found stunnel: drwxr-xr-x. 2 stunnel stunnel 60 Mar 4 16:16 /var/run/stunnel redis: drwxr-x---. 2 redis redis 4096 Oct 20 2021 /var/lib/redis gvm: drwxrwx---. 10 gvm gvm 4096 Sep 3 2024 /var/lib/gvm cst: drwxr-xr-x. 3 cst cst 4096 Aug 28 2024 /home/cst apache: drwxr-xr-x. 5 root root 4096 Apr 10 2024 /usr/share/httpd postgres: drwx------. 5 postgres postgres 4096 Feb 18 23:55 /var/lib/pgsql csa: drwxr-xr-x. 19 csa postgres 4096 Mar 22 19:52 /home/csa opensearch: drwxr-xr-x. 9 opensearch opensearch 4096 Mar 4 16:17 /usr/share/opensearch opensearch-dashboards: drwxr-xr-x. 9 opensearch-dashboards opensearch-dashboards 4096 Nov 27 22:35 /usr/share/opensearch-dashboards wazuh: drwxr-x---+ 19 root wazuh 4096 Apr 18 2023 /var/ossec tcpdump: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 / logstash: drwxr-xr-x. 14 logstash logstash 4096 Aug 19 2024 /usr/share/logstash tlog: drwxr-xr-x. 2 tlog tlog 280 Mar 21 16:03 /var/run/tlog nslcd: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 / unbound: drwxr-xr-x. 2 root root 4096 Aug 6 2024 /etc/unbound mosquitto: drwxr-xr-x. 2 root root 4096 Aug 14 2024 /etc/mosquitto setroubleshoot: drwx------. 2 setroubleshoot setroubleshoot 4096 Apr 11 2024 /var/lib/setroubleshoot tss: crw-rw-rw-. 1 root root 1, 3 Mar 4 16:22 /dev/null nscd: dr-xr-xr-x. 20 root root 4096 Mar 19 22:01 / cgm: drwxr-xr-x. 4 cgm admin 4096 Mar 18 14:29 /home/cgm	

			ccg: drwx------. 12 ccg ccg 4096 Mar 21 16:03 /home/ccg splunkfwd: drwxr-x---+ 9 splunkfwd splunkfwd 4096 Nov 29 21:26 /opt/splunkforwarder fapolicyd: drwxrwx---. 2 root fapolicyd 4096 Dec 31 13:01 /var/lib/fapolicyd pesign: Home directory not found mfe: drwxr-xr-x. 2 mfe root 4096 Mar 19 20:56 /var/McAfee/agent/ma_home	
Test 10 AC-6-1 Least Privilege: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators, AF Defined Value []				
68	Access control policy; procedures addressing least privilege; list of assigned access authorizations (user privileges); information system configuration settings and associated documentation; information system audit records; other relevant documents or records AC-6(1)1 defines security-relevant information for which access must be explicitly authorized; AC-6(1)[2]a Hardware AC-6(1)[2]b Software AC-6(1)[2]c Firmware AC-6(1)[3]a Organization defined security functions AC-6(1)[3]b Security relevant information		Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. All accounts will be given the minimum user rights required for them to perform their daily duties. TFM Group membership defines the scope of access for a given user and provides an avenue to manage least privilege and separation of duties. All access rights are granted by the IAO in conjunction with administrative authority. All users are granted access based on group membership as defined in Section 3.1.3. It is imperative that users receive adequate training and understand the access rights granted to them based on their role.	

			Administrative users have access rights that allow a broad range of privileges throughout the system. Non-administrative users have a limited scope of access rights based on the requirements of the role. Most non-administrative users have specific group membership in common providing a clear distinction between those with administrative access rights.	
Test 10 AC-6(5) Least Privilege | Privilege Accounts: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators				
69	**AC-6(5)[1]** defines personnel or roles for which privileged accounts on the information system are to be restricted; and **AC-6(5)[2]** Restricts privileged accounts on the information system to organization-defined personnel or roles.		TFM User rights and access are determined based on role and job function and enforced through group assignments using a least privilege practice. Group accounts are prohibited for shared login use. Each system has a root or administrator (privileged) account. The root account cannot be logged into directly. Users that need to perform IAO or system administration duties, including security scans and functionality, will need to log in with a standard user account before elevating to a privileged account to perform administrator tasks. Non-privileged users have no visibility into management functionality.	
Test 10 AC-6(7)A Least Privilege | Review of User Privileges: The information system: Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators, AF Defined Value []				
70	**AC-6(7)(a)1** defines roles or classes of users to which privileges are assigned **AC-6(7)(a)2** defines the frequency to review the privileges assigned to organization-defined roles or classes of users to validate the need for such		CNSS Annually, at a minimum… Not appropriate to define at the AF IC level; the ISSM/ISSO is responsible for determining the value(s) in collaboration with the appropriate office of primary responsibility and document the value(s) within the body-of-evidence. All accounts should be reviewed at a minimum every 6 months or when a staff member leaves, gets promoted, or job responsibilities change. Break Glass passwords need to be	

	privileges **AC-6(7)(a)3** reviews the privileges assigned to organization-defined roles or classes of users with the organization-defined frequency to validate the need for such privileges		changed after being used to unlock a root or administrator account. Privilege access is given by task, need-to-know, or system responsibilities. NO CHANGING OF PASSWORDS ALLOWED Review of User Privileges The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business functions, environments of operation, technologies, or threats. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions.	
Test 10 AC-6(8) Least Privilege: Privilege Levels for Code Execution: Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators; system developers, AF Defined Value []				
71	AC-6(8)1 the organization defines software that should not execute at higher privilege levels than users executing the software; and		CNSS ISSO / ISSM is responsible for determining software applications / programs which require need to execute with elevated privileges to perform required functions. The information system must prevent from executing at higher privilege levels than users executing the software. The ISSO / ISSM will work with the engineers/system administrators to assure these privileges are limited to certain users. Audit files are being tracked via SPLUNK and Nessus scans.	
72	AC-6(8)2 the information system prevents organization-defined software from executing at higher privilege levels than users executing the software. User must not be a member of SU or SUDO, try to sudo or		Access denied or not accessible Privilege users and least Privilege The following are examples of privileges restricted to administrative accounts: • Making changes to installed software packages • Accessing security logging, groups, and related information • Accessing and managing audit logs • Changing security attributes	

	su		and associating those attributes with information • Managing other user accounts By default, only a privileged account can make changes to an account with equal access. It is assumed that if a privileged account is used, the user will have total control over the system, which includes user/password management.	
Test 11 AC-6(9) Least Privilege: Auditing Use Of Privileged Functions. Organizational personnel with responsibilities for reviewing least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system/network administrators; system developers NSS Defined Value [], AF Defined Value []				
73	Determine if the information system audits the execution of privileged functions. Try to access the audit files or execute a program as root or sudo.		TFM Audited Activities Each operating system has a built-in auditing capability that is maximized to its full potential (within the scope of requirements) to capture specific user activities. The basis for designating auditing activities is derived from NIST 800-53 in conjunction with DoD-recommended values and site-specific SOP requirements. You should receive a denied or no access	
Test 11 AC-6(10) Least Privilege: Prohibits non-privileged Users From Executing Privileged Functions Organizational personnel with responsibilities for defining least privileges necessary to accomplish specified tasks; organizational personnel with information security responsibilities; system developers				
74	**AC-6(10)1** disabling implemented security safeguards/countermeasures; **AC-6(10)2** circumventing security safeguards/countermeasures; or **AC-6(10)3** altering implemented security safeguards/countermeasures			

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 []				
75	Check for the use of pam_faildelay	cat /etc/pam.d/system-auth | grep faildelay	Returns **auth optional pam_faildelay.so**	
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 []				
76	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."	
77	Verify the SSH daemon is configured for logon warning banners. From a remote system:	ssh to utility node	The output of line 60 is displayed.	
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 []				
78	Check the at pam_lastlog is used and not silent, or that the SSH daemon is configured to display last login information.	sudo cat /etc/ssh/sshd_config | grep -i lastlog	Results **#PrintLastLog yes** **PrintLastLog yes**	
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 []				
79	check idle activation, idle delay, session lock on gnome screen saver	rpm -qa | grep -i gnome	returns nothing as gnome is not installed	
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 []				
80	Review session lock visual	rpm -qa | grep -i gnome	Returns nothing as no visuals associated with gnome are installed	
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 []				

81	Determine if a publicly-viewable pattern is displayed during a session lock. Some screensaver themes, which are available but not included in the OEL (Oracle Enterprise Linux) distribution, use a snapshot of the current screen as a graphic. This theme does not qualify as a publicly-viewable pattern.	rpm -qa | grep -i gnome	Returns nothing as no visuals associated with gnome are installed	
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 []				
82	List exported filesystems:	cat /etc/exports	Nothing should be returned as there are no exported filesystems	
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 []				
83	Review remote access authorization policy and procedures.		Remote access is documented in policy and procedures.	
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 []				
84	Determine if auditing is enabled.	sudo ps -ef | grep auditd | grep -v grep	Will show similar output to below: **root 42 2 0 Mar04 ? 00:04:17 [kauditd]** **root 1089 1 0 Mar04 ? 00:55:06 /sbin/auditd**	
85	Check /etc/syslog.conf and verify the auth facility is loggin both the notice and info level messages by using one of the procedures below.	$ sudo cat /etc/rsyslog.d/cron.conf | grep 'auth\.*'	Returns: **auth.*;authpriv.*;daemon.* /var/log/secure**	
86	The system's access control program must log each system access attempt.	sudo ls /etc/rsyslog.simp.d/	Returns lists of files under the directory: 00_simp_pre_logging 00_simp_pre_logging.conf 07_simp_drop_rules	

			07_simp_drop_rules.conf 09_failover_hack 09_failover_hack.conf 15_include_default_rsyslog 15_include_default_rsyslog.conf 99_simp_local 99_simp_local.conf	
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 []				
87	Check to see if rsh/rlogin are installed.	rpm -qa | grep -i rsh	Nothing is returned as rsh is not installed. Rlogin requires rsh so you can't have one without the other.	
88	Verify the SNMP daemon uses SHA or AES for SNMPv3 users.	sudo ps -ef | grep snmp | grep -v grep	Nothing returned as snmp is not running	
89	Check the SSH daemon configuration for allowed ciphers.	sudo cat /etc/ssh/sshd_config | grep -i ciphers | grep -v '^#'	Returns **Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr**	
90	Check the SSH daemon configuration for allowed MACs.	$ sudo cat /etc/ssh/sshd_config | grep -i macs | grep -v '^#'	Returns **MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256** each entry has hmac-sha2-256 or greater	
91	Find out which LDAP is used Find name of ldap server Look for the following four lines and verify sss is being used passwd: shadow: group: netgroup:	rpm -qa | grep openldap sudo cat /etc/openldap/ldap.conf | grep -i uri sudo cat /etc/nsswitch.conf | grep -E 'passwd|shadow|group'	Returns **openldap-2.4.46** **openldap-clients-2.4.46-19.el8_10.x86_64** Returns **URI** **ldaps://utility.checkmate.phen** Returns **passwd: files [! NOTFOUND=return] sss mymachines systemd** **shadow: files [! NOTFOUND=return] sss** **group: files [! NOTFOUND=return] sss mymachines systemd** **netgroup: files [! NOTFOUND=return] sss** Returns	

	Check if NSS LDAP TLS is using only FIPS 140-2 approved cryptographic algorithms.	update-crypto-policies --show	**DEFAULT** this is TLS 1.2 and 1.3 on all RHEL 8 environments which are FIPS 140-2 approved	
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 []				
92	Check the SSH daemon configuration for listening network addresses.	sudo cat /etc/ssh/sshd_config | grep -i listen	Returns **#ListenAddress 0.0.0.0** **#ListenAddress ::** entries are commented out as no addresses are configured to listen	
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 []				
93	Check /etc/securetty for terminals authorized to transmit tokens	$ sudo cat /etc/securetty	Returns nothing as no terminals are authorized	
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**				
94	Review remote access policies and procedure		... privileged functions and security relevant information ... Secure Shell [SSH] ... 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 []				
95	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 []				
96	Review remote access control for mobile devices policy and procedures.		No mobile devices allowed.	

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 []				
97	Review use of external IS policy and procedures.		No external IS allowed	
98	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.				
99	Verify successful logins are being logged:	last -R | head -n 20	Returns the last 20 successful logins	
100	Verify if unsuccessful logons are being logged:	lastb -R | head -n 20	Returns the last 20 unsuccessful logins	
101	Check the log files to determine if access to the root account is being logged. Examine /etc/rsyslog.simp.d/* 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.	sudo cat /etc/rsyslog.simp.d/99_simp_local/ZZ_default.conf | grep authpriv	Returns ***.info;mail.none;authpriv.none;cron.none;local6.none;local5.none action(type="omfile" file="/var/log/messages")** **authpriv.*;local6.*;local5.* action(type="omfile" file="/var/log/secure")**	

102	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	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -e " cr"	Returns **-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S create_module -F key=module-change** **-a always,exit -F arch=b32 -S create_module -F key=module-change** **-a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access** **-a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access** **-a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access** **-a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access** **-a always,exit -F arch=b64 -S create_module,init_module,finit_module,delete_module -k modules** **-a always,exit -F arch=b32 -S create_module,init_module,finit_module,delete_module -k modules**	
103	Check the system audit configuration to determine if file and directory	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep	Returns **-a always,exit -F arch=b32 -S unlink,unlinkat,rename,renameat -F auid>=1000 -F auid!=unset -F**	

	deletions are audited.	-i unlink	**key=delete -a always,exit -F arch=b64 -S unlink,unlinkat,rename,renameat -F auid>=1000 -F auid!=unset -F key=delete -a always,exit -F arch=b64 -S unlink -F auid>=1000 -F auid!=4294967295 -F key=delete -a always,exit -F arch=b32 -S unlink -F auid>=1000 -F auid!=4294967295 -F key=delete -a always,exit -F arch=b64 -S unlinkat -F auid>=1000 -F auid!=4294967295 -F key=delete -a always,exit -F arch=b32 -S unlinkat -F auid>=1000 -F auid!=4294967295 -F key=delete -a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access -a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access -a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access -a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access**	
104	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	sudo cat /etc/audit/audit.rules | egrep "faillog|lastlog" | grep -P "(wa|aw)"	Returns **-w /var/log/lastlog -p wa -F key=logins -w /var/log/lastlog -p wa -k logins -w /var/log/faillog -p wa -k logins**	

	/var/log/faillog and /var/log/lastlog must be protected from tampering of the login records.			
105	Check the system's audit configuration.	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -i "chmod"	Returns **-a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S chmod -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod**	
106	Determine if the init_module syscall is audited.	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -i "init_module"	Returns **-a always,exit -F arch=b64 -S init_module -F key=module-change** **-a always,exit -F arch=b32 -S init_module -F key=module-change** **-a always,exit -F arch=b64 -S**	

			finit_module -F key=module-change -a always,exit -F arch=b32 -S finit_module -F key=module-change -a always,exit -F arch=b64 -S create_module,init_module,finit_module,delete_module -k modules -a always,exit -F arch=b32 -S create_module,init_module,finit_module,delete_module -k modules -a always,exit -F arch=b32 -S finit_module -F auid>=1000 -F auid!=unset -F key=modules -a always,exit -F arch=b32 -S init_module -F auid>=1000 -F auid!=unset -F key=modules -a always,exit -F arch=b64 -S finit_module -F auid>=1000 -F auid!=unset -F key=modules -a always,exit -F arch=b64 -S init_module -F auid>=1000 -F auid!=unset -F key=modules	
107	Depending on what system is used for log processing either /etc/syslog.conf or /etc/rsyslog.conf will be the logging configuration file.	sudo cat /etc/rsyslog.d/cron.conf | grep "cron"	Returns **cron.* /var/log/cron**	
108	Check the configured cron log file found I the cron entry of /etc/rsyslog.conf (normally /var/log/cron).	ls -l /var/log/cron	Returns similar output **-rw-r-----+ 1 root root 1413494 Mar 22 22:44 /var/log/cron**	
109	Verify the system logs martian packets.	sudo cat /proc/sys/net/ipv4/conf/all/log_martians	Returns **1** showing logging is enabled	
110	Check /etc/rsyslog.simp.d and verify the authpriv facility is logging the "info" and "mail" priority messages. Also validate TCP messages are going to /var/log/messages	sudo cat /etc/rsyslog.simp.d/99_simp_local/ZZ_default.conf | grep "authpriv.*"	Returns ***.info;mail.none;authpriv.none;cron.none;local6.none;local5.none action(type="omfile" file="/var/log/messages") authpriv.*;local6.*;local5.* action(type="omfile" file="/var/log/secure")**	
111	Check that auditd is		Returns	

	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.	sudo cat /etc/audit/audit.rules | grep -iE "eperm|eacces"	**-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access** **-a always,exit -F arch=b32 -S open,creat,truncate,ftruncate,openat,open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access** **-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access** **-a always,exit -F arch=b64 -S open,truncate,ftruncate,creat,openat,open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=unset -F key=access** **-a always,exit -F arch=b64 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S creat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S creat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S open -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S open -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S open -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S open -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b64 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S openat -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access** **-a always,exit -F arch=b32 -S openat -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access**	

			-a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b64 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b64 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b32 -S truncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b32 -S truncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b64 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b64 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b32 -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b32 -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -F key=access -a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access -a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat	

			,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access -a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access -a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access -a always,exit -F perm=a -F exit=-EACCES -k access -a always,exit -F perm=a -F exit=-EPERM -k access -S openat -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access -a always,exit -F arch=b64 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access -a always,exit -F arch=b32 -S open_by_handle_at -F exit=-EACCES -F auid>=1000 -F auid!=unset -F key=access	
112	Check the system audit configuration to determine if file and directory deletions are audited.	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -i "rmdir"	Returns -a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete -a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete -a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EACCES -k access -a always,exit -F arch=b64 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,rename,renameat,truncate,ftruncate,rmdir,unlink,unlinkat -F exit=-EPERM -k access -a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdirat,mknodat,linkat,symlinkat,openat,open_by_handle_at,open,close,renam	

			e,renameat,truncate,ftruncate,rmdir ,unlink,unlinkat -F exit=-EACCES -k access -a always,exit -F arch=b32 -S creat,mkdir,mknod,link,symlink,mkdi rat,mknodat,linkat,symlinkat,openat ,open_by_handle_at,open,close,renam e,renameat,truncate,ftruncate,rmdir ,unlink,unlinkat -F exit=-EPERM -k access -a always,exit -F arch=b32 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete -a always,exit -F arch=b64 -S rmdir -F auid>=1000 -F auid!=unset -F key=delete	
113	Check the system's audit configuration for changing mode.	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -i "fchmod"	Returns -a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid! =unset -F key=perm_mod -a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid! =unset -F key=perm_mod -a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid! =unset -F key=perm_mod -a always,exit -F arch=b32 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid! =unset -F key=perm_mod -a always,exit -F arch=b64 -S fchmod -F auid>=1000 -F auid!=unset -F key=perm_mod	
114	Check the system's audit configuration relative to a directory file descriptor.	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -i "fchmodat"	Returns -a always,exit -F arch=b32 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S chmod,fchmod,fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod	

			-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod **-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S fchmodat -F auid>=1000 -F auid!=unset -F key=perm_mod**	
115	Check the system's audit configuration relative to changing file ownership. Confirm fchown, lchown, and fchownat are included.	sudo cat /etc/audit/audit.rules | grep -e "-a always,exit" | grep -i "chown"	Returns **-a always,exit -F arch=b32 -S lchown,fchown,chown,fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S chown,fchown,lchown,fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=4294967295 -F key=perm_mod** **-a always,exit -F path=/usr/libexec/pt_chown -F perm=x -F auid>=1000 -F auid!=4294967295 -F key=setuid/setgid** **-a always,exit -F arch=b64 -S chown,fchown,fchownat,lchown -k chown** **-a always,exit -F arch=b32 -S chown,fchown,fchownat,lchown -k chown** **-a always,exit -F arch=b32 -S chown -F auid>=1000 -F auid!=unset -F**	

			key=perm_mod -a always,exit -F arch=b32 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b32 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b32 -S lchown -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S chown -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S fchownat -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S fchown -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S lchown -F auid>=1000 -F auid!=unset -F key=perm_mod	
116	Check the system's audit configuration for setting extended attributes.	sudo cat /etc/audit/audit.rules | grep setxattr	Returns **-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod -a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod -a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod -a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod -a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod -a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=4294967295 -F key=perm_mod -a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -k attr -a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,removexattr,lremovexattr,fremovexattr -k**	

			attr **-a always,exit -F arch=b32 -S fsetxattr -F auid=0 -F key=perm_mod** **-a always,exit -F arch=b32 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S lsetxattr -F auid=0 -F key=perm_mod** **-a always,exit -F arch=b32 -S lsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b32 -S setxattr -F auid=0 -F key=perm_mod** **-a always,exit -F arch=b32 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S fsetxattr -F auid=0 -F key=perm_mod** **-a always,exit -F arch=b64 -S fsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S lsetxattr -F auid=0 -F key=perm_mod** **-a always,exit -F arch=b64 -S lsetxattr -F auid>=1000 -F auid!=unset -F key=perm_mod** **-a always,exit -F arch=b64 -S setxattr -F auid=0 -F key=perm_mod** **-a always,exit -F arch=b64 -S setxattr -F auid>=1000 -F auid!=unset -F key=perm_mod**	
117	Determine if the delete_module syscall is audited.	sudo cat /etc/audit/audit.rules | grep -i "delete_module"	Returns **-a always,exit -F arch=b64 -S delete_module -F key=module-change** **-a always,exit -F arch=b32 -S delete_module -F key=module-change** **-a always,exit -F arch=b64 -S create_module,init_module,finit_module,delete_module -k modules** **-a always,exit -F arch=b32 -S create_module,init_module,finit_module,delete_module -k modules** **-a always,exit -F arch=b32 -S delete_module -F auid>=1000 -F auid!=unset -F key=modules** **-a always,exit -F arch=b64 -S delete_module -F auid>=1000 -F auid!=unset -F key=modules**	
118	Determine if insmod, modprobe, and rmmod are audited.	sudo cat /etc/audit/audit.rules | grep -E "insmod|modprobe|rmmod"	Returns **-w /usr/sbin/insmod -p x -F auid!=4294967295 -F key=module-change** **-w /sbin/insmod -p x -F auid!=4294967295 -F key=module-change** **-w /usr/sbin/rmmod -p x -F auid!=4294967295 -F key=module-change** **-w /sbin/rmmod -p x -F auid!**	

			=4294967295 -F key=module-change -w /usr/sbin/modprobe -p x -F auid! =4294967295 -F key=module-change -w /sbin/modprobe -p x -F auid! =4294967295 -F key=module-change -w /usr/sbin/insmod -p x -k modules -w /sbin/insmod -p x -k modules -w /usr/sbin/rmmod -p x -k modules -w /sbin/rmmod -p x -k modules -w /usr/sbin/modprobe -p x -k modules -w /sbin/modprobe -p x -k modules -w /etc/modprobe.conf.d -p wa -k CFG_sys -w /etc/modprobe.d/00_simp_blacklist.c onf -p wa -k CFG_sys	
119	Check the system's audit configuration tracks the removal of extended attributes.	sudo cat /etc/audit/audit.rules | grep -i "removexattr"	Return **-a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,remove xattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,remove xattr,lremovexattr,fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid! =4294967295 -F key=perm_mod -a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid! =4294967295 -F key=perm_mod -a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid! =4294967295 -F key=perm_mod -a always,exit -F arch=b32 -S fremovexattr -F auid>=1000 -F auid! =4294967295 -F key=perm_mod -a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid! =4294967295 -F key=perm_mod -a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid! =4294967295 -F key=perm_mod -a always,exit -F arch=b64 -S setxattr,lsetxattr,fsetxattr,remove xattr,lremovexattr,fremovexattr -k attr -a always,exit -F arch=b32 -S setxattr,lsetxattr,fsetxattr,remove xattr,lremovexattr,fremovexattr -k attr -a always,exit -F arch=b32 -S fremovexattr -F auid=0 -F key=perm_mod -a always,exit -F arch=b32 -S**	

			fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b32 -S lremovexattr -F auid=0 -F key=perm_mod -a always,exit -F arch=b32 -S lremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b32 -S removexattr -F auid=0 -F key=perm_mod -a always,exit -F arch=b32 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S fremovexattr -F auid=0 -F key=perm_mod -a always,exit -F arch=b64 -S fremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S lremovexattr -F auid=0 -F key=perm_mod -a always,exit -F arch=b64 -S lremovexattr -F auid>=1000 -F auid!=unset -F key=perm_mod -a always,exit -F arch=b64 -S removexattr -F auid=0 -F key=perm_mod -a always,exit -F arch=b64 -S removexattr -F auid>=1000 -F auid!=unset -F key=perm_mod	
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 []				
120	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 []				
121	The /etc/xinetd.conf file and each file in the /etc/xinetd.d directory file should be examined for the following:	sudo ps -ef | grep xinetd | grep -v grep	No results are returned as xinetd is not running.	
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, the				

audit records include: 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, entity that completed the event/action . . .				
122	Review the content of the audit records	sudo cat /var/log/audit/audit.log | head -n 20	The last 20 messages containing a 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 are displayed.	
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.				
123	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.	sudo cat /boot/efi/EFI/redhat/grub.cfg | grep "audit" | grep -v "^#"	Returns **set kernelopts="root=/dev/mapper/VolGroup00-RootVol ro crashkernel=auto resume=/dev/mapper/VolGroup00-SwapVol rd.lvm.lv=VolGroup00/RootVol rd.lvm.lv=VolGroup00/SwapVol rhgb quiet audit=1 transparent_hugepage=never fips=0 boot=UUID=810c8e15-b13e-4a61-9ae6-ca1bd392e368 pti=on page_poison=1 slub_debug=P audit_backlog_limit=8192 no5lvl "**	

124	Ensure the Kernel auditing is active.	sudo cat /etc/audit/plugins.d/syslog.conf	Returns
			**# This File is managed by Puppet
			#
			# This file controls the configuration of the syslog plugin.
			active = yes
			direction = out
			path = /sbin/audisp-syslog
			type = always
			args = LOG_INFO LOG_LOCAL5
			format = string**	

125	Ensure all audit records are forwarded to a remote server.	sudo cat /etc/rsyslog.d/remote.conf | grep '@'| grep "*.*" | grep -v "^#"	Returns the IP of the remote server configured	
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 []				
126	Review audit storage capacity policy		Storage capacity is allocated	

	and procedures.			
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				
127	Verify the /etc/audit/auditd.conf has the disk_full_action and disk_error_actions parameters set.	sudo cat /etc/audit/auditd.conf | grep -E "disk_full_action|disk_error_action"	Returns **disk_full_action = syslog** **disk_error_action = syslog**	
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 []				
128	Check /etc/audit/auditd.conf for the space_left_action and action_mail_acct parameters.	sudo cat /etc/audit/auditd.conf | grep -E "space|action_mail"	Returns **space_left = 25%** **space_left_action = email** **admin_space_left = 50** **admin_space_left_action = rotate** **action_mail_acct = root**	
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 []				
129	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 []				
130	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 []				
131	Verify the time is accurate	date	Time is displayed in UTC	
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.				
132	Check if NTP running: Confirm the timeservers and	$ sudo ps -ef | grep chronyd | grep -v grep cat	Returns **chrony 1470 1 0 Mar04 ? 00:00:00 /usr/sbin/chronyd** Returns the configuration for time.	

	peers or multicast client (as applicable) are local or authoritative U.S. DoD sources appropriate for the level of classification which the network operates.	/etc/chrony.conf	Since this the utility node the NTP server section will only show **server utility maxpoll 16** as it is the source.	
133	Check crontabs for the jobs running via cron	cat /etc/cron.d/*	Returns **# Run the hourly jobs** **SHELL=/bin/bash** **PATH=/sbin:/bin:/usr/sbin:/usr/bin** **MAILTO=root** **01 * * * * root run-parts /etc/cron.hourly** **cat: /etc/cron.d/aide: Permission denied** **0,30 * * * * root /opt/McAfee/agent/scripts/ma checkhealth >/dev/null 2>/dev/null** **# Run system wide raid-check once a week on Sunday at 1am by default** **0 1 * * Sun root /usr/sbin/raid-check**	
134	Check the Chrony daemon configuration for at least two external servers.	cat /etc/chrony.conf	As this is the timesource there will be no external servers it connects to for time sync.	
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 []				
135	Perform the following to determine the location of audit logs and then check the ownership.	sudo cat /etc/audit/auditd.conf | grep "log_file = /" sudo ls -l /var/log/audit/audit.log	Returns **log_file = /var/log/audit/audit.log** Returns **-rw-------+ 1 root root 6734212 Mar 23 00:29 /var/log/audit/audit.log**	
136	Verify the audit tool executables are owned by root.	ls -l /sbin/ | grep -E "auditctl| auditd|ausearch| aureport|autrace"	Returns **-rwxr-x---. 1 root root 46120 Sep 12 2024 auditctl** **-rwxr-x---. 1 root root 155360 Sep 12 2024 auditd** **-rwxr-x---. 1 root root 125288 Sep 12 2024 aureport** **-rwxr-x---. 1 root root 133488 Sep 12 2024 ausearch** **-rwxr-x---. 1 root root 16936 Sep 12 2024 autrace**	
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 []				
137	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 []				
138	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.				
139	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 []				
140	Determine if auditing is enabled.	sudo ps -ef | grep auditd | grep -v grep	Returns **root 42 2 0 Mar04 ? 00:04:21 [kauditd]** **root 1089 1 0 Mar04 ? 00:55:48 /sbin/auditd**	
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 []				
141	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 []				
142	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 []				
143	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 []				
144	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 []				
145	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;				
146	Review baseline configuration policies and procedures		. . . a list of software authorized to execute on the information system which includes only that software evaluated and approved by	

			the ISSO/ISSM with the local CCB	
Test 51 CM-6 Configuration Settings: The organization: a. Establishes and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. NSS Defined Value [], AF Defined Value a. . . the latest STIGS, SNAC, USGCB guidance and AF ISR configuration guides . . .				
147	Verify the system will not log in accounts with blank passwords.	sudo cat /etc/pam.d/system-auth | grep null	No entry for nullok is found as the system doesn't allow blank passwords	
148	Check for the existence of the files to see if remote hosts are configured. .rhosts .shosts hosts.equiv shosts.equiv	sudo find / -type f \(-name ".rhosts" -o -name ".shosts" -o -name "hosts.equiv" -o -name "shosts.equiv" \) 2>/dev/null	Nothing returns as there are no remote hosts configured	
149	Check for an enable "debug" command provided by the SMTP service.	cat /etc/postfix/main.cf | grep debug_peer_list	Returns **# matches a pattern in the debug_peer_list parameter.** **# The debug_peer_list parameter specifies an optional list of domain** **#debug_peer_list = 127.0.0.1** **#debug_peer_list = some.domain** Items commented out as debug not enabled	
150	Determine if the system is configured to boot from devices other than the system startup media.	Validate through bios boot order	No alternative boot devices	
151	Determine if the system uses the GRUB boot loader;	sudo ls -l /boot/efi/EFI/redhat/grub.cfg	Results **-rwx------. 1 root root 6630 Mar 23 02:28 /boot/efi/EFI/redhat/grub.cfg** proving the system uses the GRUB boot loader	
152	Verify that reboot using the CTRL-ALT- the string is commented out DELETE	systemctl get-default	Returns **multi-user.target** showing ctrl-alt-del.target is not used and thus disabled	

	key sequence has been disabled			
153	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				
154	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				
155	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 []				
156	Logging should be enabled for those types of file systems not turning on logging by default.	df -hT	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.	
157	Verify local filesystems use.	cat /proc/mounts | grep -E "ext4|xfs"	Returns **/dev/mapper/VolGroup00-RootVol / ext4 rw,seclabel,relatime 0 0** **selinuxfs /sys/fs/selinux selinuxfs rw,relatime 0 0** **/dev/mapper/VolGroup00-RootVol /tmp ext4 rw,seclabel,nosuid,nodev,noexec,relatime 0 0** **/dev/mapper/VolGroup01-HomeVol /home ext4 rw,seclabel,nosuid,nodev,noexec,relatime,i_version 0 0** **/dev/sda2 /boot ext4 rw,seclabel,nosuid,nodev,relatime 0 0** **/dev/mapper/VolGroup00-VarVol /var ext4 rw,seclabel,nodev,relatime 0 0**	

			/dev/mapper/VolGroup00-RootVol /var/tmp ext4 rw,seclabel,nosuid,nodev,noexec,relatime 0 0 /dev/mapper/VolGroup00-VarLogVol /var/log ext4 rw,seclabel,nosuid,nodev,noexec,relatime 0 0 /dev/mapper/VolGroup00-VarLogAuditVol /var/log/audit ext4 rw,seclabel,nosuid,nodev,noexec,relatime 0 0 /dev/mapper/VolGroup00-VarLogVol /home/csa/log ext4 rw,seclabel,nosuid,nodev,noexec,relatime 0 0 /dev/mapper/VolGroup00-VarLogVol /var/ossec/logs ext4 rw,seclabel,nosuid,nodev,noexec,relatime 0 0 /dev/mapper/VolGroup01-OptVol /opt ext4 rw,seclabel,nodev,relatime 0 0	
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 []				
158	Check the system for duplicate account names.	cat /etc/passwd | cut -d: -f1 | sort | uniq -d	Nothing is returned as there are no duplicate names	
159	Perform the following to ensure there are no duplicate UIDs:	cat /etc/passwd | cut -d: -f3 | sort | uniq -d	Nothing is returned as there are no duplicate UIDs	
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 []				
162	Review multifactor authentication for privileged accounts	sudo cat /etc/sssd/sssd.conf | grep mfa	Nothing returns as mfa not enabled on the system	
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 []				
163	Review multifactor authentication for privileged accounts	sudo cat /etc/sssd/sssd.conf | grep mfa	Nothing returns as mfa not enabled on the system	
164	To determine how the SSH daemon's "HostbasedAuthentication" option is set, run the following command: If no line, a commented line, or a	sudo cat /etc/ssh/sshd_config | grep -i HostbasedAuthentication	Returns **#HostbasedAuthentication no HostbasedAuthentication no # HostbasedAuthentication** showing host based authentication is disabled	

	line indicating the value "no" is returned, then the required value is set.			
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 []				
165	Review multifactor authentication for privileged accounts	sudo cat /etc/sssd/sssd.conf | grep mfa	Nothing returns as mfa not enabled on the system	
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 []				
166	Review multifactor authentication for privileged accounts	sudo cat /etc/sssd/sssd.conf | grep mfa	Nothing returns as mfa not enabled on the system	
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				
167	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				
168	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 []				
169	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 []				
170	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 []				
171	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 []				
172	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 []				
173	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 []				
174	Check the minimum time period between password changes for each user account is 1 day.	sudo cat /etc/login.defs | grep PASS_MIN_DAYS	Returns **PASS_MIN_DAYS 1**	
175	Check the system password length setting. Check the password minlen option	sudo cat /etc/security/pwquality.conf | grep minlen	Results **minlen = 15**	

	Confirm the minlen option is set to at least 15 as in the example below: password required minlen=15			
176	Verify no valid password hash in /etc/passwd or /etc/shadow begins with a character other than an underscore (_) or dollar sign ($). When a password has is found, verify it starts with 5 or 6	sudo cat /etc/passwd sudo cat /etc/shadow | cut -d ':' -f2	Results contents of passwd are shown with no password hashes Results Disabled accounts have !!, system accounts will have * and passwords will start with 5 or 6	
177	Check the ucredit setting to verify at password complexity	$ sudo cat /etc/security/pwquality.conf | grep credit	Result **dcredit = -1** **ucredit = -1** **lcredit = -1** **ocredit = -1**	
178	Check the max days field (the 5th field) of /etc/shadow.	sudo cat /etc/shadow | awk -F: '{print $1 " " $5}'	Result the username and maximum days a password is valid is displayed	
179	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	
180	Check That passwords require different characters from past passwords	sudo cat /etc/security/pwquality.conf | grep difok	Result **difok = 8**	
181	Verify /etc/security/opasswd is present verify the remember option is 5 or greater in system-	ls /etc/security/opasswd sudo cat /etc/pam.d/system-auth | grep	Result **/etc/security/opasswd** Result **password required pam_pwhistory.so use_authtok remember=24 retry=1**	

	auth	remember	**enforce_for_root**	
182	Determine if root has logged in over an unencrypted network connection. Look for any lines that do not have sshd as the associated service.	sudo cat /var/log/secure | grep "sshd.*root" sudo cat /var/log/messages | grep "sshd.*root"	No results will be displayed as root is not an account that can login	
183	Verify no password hashes are present in /etc/passwd.	cut -d : -f 2 /etc/passwd | egrep -v '^(x|*)$'	Nothing is returned as there are no passwords in the file	
184	Check the system for the existence of any .netrc files.	sudo find / -name .netrc -print 2>/dev/null	No results returned as there are no .netrc files	
185	Determine if default system accounts (such as those for sys, bin, uucp, nuucp, daemon, smtp) have been disabled. If an account's password field is "*", "*LK*", or is prefixed with a '!', the account is locked or disabled.	sudo cat /etc/shadow | awk -F: '{print $1 " " $2}'	Result the user and password fields are displayed to verify which accounts are disabled	
186	The telnet service included in the OEL 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.	rpm -qa | grep telnet	Nothing is returned as telnet is not installed therefore it can’t run	

	Check if telnetd is running:			
187	Verify LDAP is running on the system.	systemctl status slapd	Returns **slapd.service - OpenLDAP Server Daemon** **Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)** **Active: active (running) since Wed 2025-01-29 03:43:35 UTC; 11h ago** **Docs: man:slapd** **man:slapd-config** **man:slapd-hdb** **man:slapd-mdb** **file:///usr/share/doc/openldap-servers/guide.html** **Main PID: 3285569** **Tasks: 10 (limit: 100608)** **Memory: 87.5M** **CGroup: /system.slice/slapd.service** **└─3285569 /usr/sbin/slapd -u ldap -h ldap:/// ldaps:/// ldapi:///**	
188	Verify the system-auth settings are being applied. The file ls -l /etc/pam.d/system-auth" is auto-generated by "authconfig". Any manual changes made to it will be lost next time "authconfig" is run. Check to see if the system's default of the symlink ls -l /etc/pam.d/system-auth" pointing to /etc/pam.d/system-auth" has been changed. If the symlink points to "/etc/pam.d/system-auth", manual changes cannot be protected. This is a finding.	ls -l /etc/pam.d/system-auth	Returns: **lrwxrwxrwx. 1 root root 27 Feb 18 23:32 /etc/pam.d/system-auth -> /etc/authselect/system-auth**	

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 []				
189	This system does not utilize PKI-based 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 []				
190	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 []				
191	Log out of the system		User is logged out	
192	Log into of 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 []				
193	Verify the algorithm used for password hashing is of the SHA-2 family.	sudo cat /etc/login.defs | grep -i "encrypt_method" sudo cat /etc/libuser.conf | egrep "crypt_style"	Returns **ENCRYPT_METHOD SHA512** Returns **crypt_style = 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 []				
194	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 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 []				
195	Review System Security Plan policies and procedures		. . . annually or as required due to system modifications	
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 []				
196	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 []				
197	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 []				
198	Review allocation of resources		Information managed using a system development life cycle mythology as identified in CCG's ISO 9001 processes.	
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 []				
199	Review life cycle support		Information managed using a system development life cycle mythology as identified in CCG's ISO 9001 processes.	
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 []				
200	Review acquisitions policies and procedures		- 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 []				
201	Review acquisitions policies and procedures			
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 []				
202	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 []				
203	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 []				
204	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 []				
205	207 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 []				
206	Review security engineering principles			
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 []				
207	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 []				
208	Review external information system Chief Information Officer		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 []				
209	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 []				
210	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:	sudo cat /etc/aide.conf sudo cat /var/log/aide/aide.log	Result The contents of the advanced intrusion detection environment are displayed. Result The contents of the log file are displayed. If there are no package discrepencies it will be empty.	
211	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 []				
212	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 []				
213	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 []				
214	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 []				

215	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 []				
216	Review information in shared resources		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 []	
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 []				
217	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	
218	Verify the system configured to use TCP syncookies when experiencing a TCP SYN flood.	$ cat /proc/sys/net/ipv4/tcp_syncookies	Result **1** showing it is enabled	
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 []				
219	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 []				

220	Verify iptables is in use	sudo cat /etc/sysconfig/iptables	Result the contents of iptables is displayed	
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 []				
221	Review boundary protection			
Test 99 SC-7 (2) Boundary Protection: The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices. NSS Defined Value [], AF Defined Value []				
222	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 []				
223	Verify firewall is enabled	systemctl status iptables	Result **● iptables.service - IPv4 firewall with iptables Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: disabled) Active: active (exited) since Tue 2025-03-04 16:16:04 UTC; 2 weeks 4 days ago Main PID: 1138 (code=exited, status=0/SUCCESS) Tasks: 0 (limit: 202766) Memory: 0B CGroup: /system.slice/iptables.service**	
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 []				
224	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 []				
225	Check the firewall rules for a default	sudo iptables --list | grep -i drop	Result **DROP udp -- anywhere**	

	deny rule to block all non designated traffic.		**anywhere multiport dports netbios-ns /* SIMP: */ DROP all -- 127.0.0.0/8 anywhere /* SIMP: */ DROP all -- anywhere anywhere PKTTYPE = broadcast /* SIMP: */ DROP all -- anywhere anywhere ADDRTYPE match src-type MULTICAST /* SIMP: */ DROP all -- anywhere anywhere /* SIMP: */ Chain LOG-DROP (0 references) DROP all -- anywhere anywhere /* SIMP: */**	
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 []				
226	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 []				
227	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 []**				
228	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 []				
229	Determine if the system is using a local firewall.	systemctl status iptables	Result **• iptables.service - IPv4 firewall with iptables**	

			Loaded: loaded (/usr/lib/systemd/system/iptables.service; enabled; vendor preset: disabled) **Active: active (exited) since Tue 2025-03-04 16:16:04 UTC; 2 weeks 4 days ago**	
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 . . .				
230	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 []				
231	Review boundary protection			
Test 110 SC-8 Transmission Integrity: The information system protects the integrity of transmitted information. NSS Defined Value [], AF Defined Value []				
232	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 []				
233	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 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 []				
234	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 []				
235	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 []				
236	Review network disconnect policies	Echo $TMOUT	Result **900**	

	and procedures		15 minutes of idle time before logout	
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.				
237	Review trusted path policies and procedures		... at a minimum, information system authentication and reauthentication.	
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 []				
238	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 []				
239	Review use of cryptography	sudo cat /etc/ssh/sshd_config | grep -iE "ciphers|kexalgorithms|macs"	Results **# Ciphers and keying** **# Ciphers, MACs, KexAlgoritms and GSSAPIKexAlgorithsm will not have any** **Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr** **KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256** **MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256**	
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 []				
240	Review public access protections			
Test 119 SC-15 Collaborating Computing Devices: The information system: a. Prohibits [Assignment: organization-defined exceptions where remote activation is to be allowed]; b. Provides physical indication of use to users physically present at the collaborating computing devices. NSS Defined Value: Remote activation of centrally managed dedicated VTC suites located in approved VTC locations, AF Defined Value []				
241	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 []				
242	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 []				
243	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.				
244	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.				
245	Review public key infrastructure certificates	openssl x509 -in /etc/pki/tls/certs/ca-bundle.crt -text -noout	Result Certificate information is displayed	
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 []				
246	Review mobile code		No mobile code	
Test 125 SC-18 (1) Mobile Code: The information system implements detection and action mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary. NSS Defined Value [], AF Defined Value []				
247	Review mobile code		No mobile code	
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 []				
248	Review mobile code. The appliance contains no 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 []				
249	Review mobile code The appliance contains no 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 []				
250	Review mobile code			

	The appliance contains no mobile code			
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 []				
251	Review voice over Internet Protocol	netstat -tuln | grep -E ":5060|:5061: (10000-20000)"	Nothing is returned as the SIP and RTPM ports used for voip are not listening	
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 []				
252	Review Secure Name / Address Resolution Service Authoritative Source) policies	cat /etc/resolv.conf	Result Local nameservers are listed	
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 []				
253	Review Secure Name / Address Resolution Service(Authoritative Source) policies and procedures	cat /etc/resolv.conf	Result Local nameservers are listed	
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 []				
254	Review Secure Name / Address Resolution Service(Authoritative Source) policies	cat /etc/resolv.conf	Result Local nameservers are listed	
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 []				
255	Review Secure Name / Address Resolution Service (Authoritative Source) policies	cat /etc/resolv.conf	Result Local nameservers are listed	
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 []				
256	Review Architecture And Provisioning For Name / Address Resolution Service	cat /etc/resolv.conf	Result Local nameservers are listed	
Test 135 SC-23 Session Authenticity: The information system provides mechanisms to protect the authenticity of communications sessions. NSS Defined Value [], AF Defined Value []				
257	Review Session Authenticity	ls -l /etc/ssh/ssh_host_*_key	Result **-rw-------. 1 root root 492 Apr 18 2023 /etc/ssh/ssh_host_ecdsa_key** **-rw-------. 1 root root 387 Apr 18 2023 /etc/ssh/ssh_host_ed25519_key** **-rw-------. 1 root root 6653 Oct 22 17:20 /etc/ssh/ssh_host_rsa_key**	
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 []				
258	Review Session Authenticity	Perform a logon and logoff of the system	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 []				
259	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 []				
260	Review Session Authenticity	sudo cat /etc/pam.d/* | grep "pam_limits"	Result **session required pam_limits.so** **session required pam_limits.so** **session required pam_limits.so** **session required pam_limits.so** **session required pam_limits.so** **session required pam_limits.so**	
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.				
261	Review session authenticity policies and procedures	openssl rand -hex 16	.Result a 32 character string is presented. 32 hex characters = 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 [] ... 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 []				
262	Review fail in known state policies and procedures		... 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 []				
263	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 system's 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 []				
264	Determine if the /home path is a separate filesystem.	grep /home /etc/fstab	Result **/dev/mapper/VolGroup01-HomeVol /home ext4 nosuid,noexec,nodev,iversion 1 2** **/var/log/csa /home/csa/log/ none defaults,bind 0 0**	
265	Determine if the /var path is a separate filesystem.	grep /var /etc/fstab	Result **/dev/mapper/VolGroup00-VarVol /var ext4 nodev 1 2** **/dev/mapper/VolGroup00-VarLogVol**	

			/var/log ext4 nosuid,noexec,nodev 1 2 **/dev/mapper/VolGroup00-VarLogAuditVol /var/log/audit ext4 nosuid,noexec,nodev 1 2** **/tmp /var/tmp none bind,nodev,noexec,nosuid 0 0** **/var/log/ossec /var/ossec/logs/ none defaults,bind 0 0** **/var/run/ossec /var/ossec/var/run/ none defaults,bind 0 0** **/var/log/csa /home/csa/log/ none defaults,bind 0 0**	
266	Determine if the /var/log/audit path is a separate filesystem.	$ grep /var/log/audit /etc/fstab	Result **/dev/mapper/VolGroup00-VarLogAuditVol /var/log/audit ext4 nosuid,noexec,nodev 1 2**	
267	Determine if the /tmp path is a separate filesystem.	$ egrep "/tmp /etc/fstab	Result **/tmp /tmp none bind,nodev,noexec,nosuid 0 0** **/tmp /var/tmp none bind,nodev,noexec,nosuid 0 0**	
268	Ask the SA if this is an NMS server.	No commands to run	This is not an NMS server.	
269	Check to see if the system is a router:	$ chkconfig --list | grep ion | egrep "(ospf|route|bgp|zebra|quagga)"	No non-routing services.	
270	Ask the SA if the system boots from removable media. If so, ask if the boot media is secured in a secure container when not in use.		It does not.	
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 []				
271	Verify antivirus is installed	rpm -qa | grep -i mcafee	Result Mcafee packages are shown to be installed	
272	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	sudo cat /var/spool/cron/* | grep oscap	Returns **15 2 * * 5 /usr/bin/oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_stig --results-arf /tmp/arf.xml --report /root/report.html /usr/share/xml/scap/ssg/content/ssg-ol8-ds.xml >**	

	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:		**/home/csa/log/cron/oscap.out 2>&1**	
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 []				
273	Review Malicious Code Protection	sudo ps -ef | grep -i mcafee	Result processes showing mcafee running are displayed providing 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 []				
274	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.	
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; b. 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; c. 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 d. 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 [] ... 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 []**				

275	# ps -ef | grep <hbss agent>	systemctl | grep nessus systemctl status nessusagent.service	**Result** **nessusagent.service loaded active running** Result **● nessusagent.service - The Nessus Client Agent** **Loaded: loaded (/usr/lib/systemd/system/nessusagent.service; enabled; vendor preset: disabled)** **Active: active (running) since Fri 2025-01-24 18:18:04 UTC; 4 days ago** **Main PID: 2675** **Tasks: 11 (limit: 100608)** **Memory: 68.1M** **CGroup: /system.slice/nessusagent.service** **├─2675 /opt/nessus_agent/sbin/nessus-service -q** **├─2683 nessusd -q** **└─2689 /opt/nessus_agent/sbin/nessus-agent-module -q**	
276	Ask the SA or IAO if a host-based intrusion detection application is loaded on the system. The preferred intrusion detection system is Trellix HBSS available through Cybercom.		HBSS	
277	Another host-based intrusion detection application, such as SELinux, may be used on the system.	getenforce	Result **Enforcing** showing selinux is enabled	
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 []				
278	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.				

279	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.	
280	Check permission on IPfilter settings	ls -l /etc/sysconfig/iptables	Result **-rw-r-----. 1 root root 5834 Jan 22 12:06 /etc/sysconfig/iptables**	
281	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 [] ... incident response personnel ... the least disruptive action to terminate suspicious events as determined appropriate for the individual system.				
282	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.	
283	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 []				
284	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 []				
285	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 []				

286	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				
287	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 []				
288	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 []				
289	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 []				

290	If the system uses sendmail examine the configuration files.
	
	Determine if sendmail only binds to loopback addresses by examining the "DaemonPortOptions" configuration options
		netstat -lnt | grep 25
		
		grep inet_interfaces /etc/postfix/main.cf
			Result
			tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN
			
			Result
			**# The inet_interfaces parameter specifies the network interface
			#inet_interfaces = all
			#inet_interfaces = $myhostname
			#inet_interfaces = $myhostname, localhost
			inet_interfaces = 127.0.0.1
			# the address list specified with the inet_interfaces parameter.
			# receives mail on (see the inet_interfaces parameter).
			# to $mydestination,**	

		grep smtpd_client_restrictions /etc/postfix/main.cf	**$inet_interfaces or $proxy_interfaces.** **# - destinations that match $inet_interfaces or $proxy_interfaces,** **# unknown@[$inet_interfaces] or unknown@[$proxy_interfaces] is returned** Result **smtpd_client_restrictions = permit_mynetworks,reject**	
Test 160 SI-8 (1) Spam Protection: The organization centrally manages spam protection mechanisms. NSS Defined Value [], AF Defined Value []				
291	(N/A since mail is not used on the system and throughout the DCGS 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 []				
292	(N/A since mail is not used on the system and throughout the DCGS enterprise)			
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 []				
293	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.	
294	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 []				
295	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 [] ... sensitive or potentially harmful information.				

296	Check the mode of log files.	stat --format="%A %a %n" /var/log/*.log	Result log files and their modes are displayed	
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 []				
297	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	