Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	**CSO-STD-1418**
Office Instruction Title:	**Red Hat Enterprise Linux 5 Server Configuration Standard**
Revision Number:	**1.0**
Effective Date:	**December 1, 2013**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PST**
Summary of Changes:	CSO-STD-1418, "Red Hat Enterprise Linux 5 Server Configuration Standard" provides the minimum configuration settings that must be applied to NRC servers running Red Hat Enterprise Linux 5 operating systems.
Training:	As requested
ADAMS Accession No.:	**ML13178A066**

Approvals				
Primary Office Owner	Policies, Standards, and Training		**Signature**	**Date**
Standards Working Group Chair	Bill Dabbs		**/RA/**	8/03/2013
Responsible SITSO	Kathy Lyons-Burke		**/RA/**	7/30/2013
DAA for Non-Major IT Investments	Director, CSO	Tom Rich	**/RA/**	7/30/2013
	Director, OIS	Jim Flanagan	**/RA/**	7/31/2013

TABLE OF CONTENTS

1 PURPOSE 1
2 GENERAL REQUIREMENTS 1
2.1 DEVIATION REQUEST PROCESS 1
3 SPECIFIC REQUIREMENTS 2
3.1 REQUIREMENTS THAT ARE DIFFERENT FROM THE CIS BENCHMARK 2
4 DEFINITIONS 211
5 ACRONYMS 233

Computer Security Standard
CSO-STD-1418

Red Hat Enterprise Linux 5 Server Configuration Standard

1 PURPOSE

CSO-STD-1418, "Red Hat® Enterprise Linux® 5 Server Configuration Standard," provides required configuration settings for the Nuclear Regulatory Commission (NRC) servers running the Red Hat Enterprise Linux (RHEL) 5 operating system.[1] These settings serve to minimize the probability of NRC sensitive information compromise. The standard applies to systems used to process Sensitive Unclassified Non-Safeguards Information (SUNSI) or Safeguards Information (SGI).

This configuration standard is intended to be used by system administrators and information system security officers (ISSOs) that have the required knowledge, skills, and abilities to apply configuration settings to RHEL 5 operating systems. RHEL 5 servers must meet all federally mandated and NRC-defined security requirements.

2 GENERAL REQUIREMENTS

All NRC servers running the RHEL 5 operating system that are owned, managed, and/or operated by the NRC or by other parties on behalf of the NRC must comply with this standard as a minimum set of controls. Additional controls may be required after a system risk analysis is completed.

RHEL 5 server installations operated by the NRC or other parties on behalf of the NRC must comply with the Center for Internet Security (CIS) RHEL 5 Benchmark, as modified by the settings/requirements provided in this standard and with the overarching requirements stated in CSO-STD-1101, "UNIX and Linux Server Security Configuration Standard." Section 3 of this standard explains how specific requirements within the CIS Benchmark are amended by NRC-specific requirements. The effective version of the CIS Benchmark is specified on the Computer Security Office (CSO) Standards web page.

2.1 Deviation Request Process

There may be circumstances when a specific configuration requirement cannot be met because of technical system limitations, business process impact, or cost-risk analysis. Implementations that do not meet this minimum configuration standard must obtain deviation approval using the CSO Deviation Request (DR) process.

---

[1] Red Hat and Enterprise Linux are registered trademarks of Red Hat, Inc.

3 SPECIFIC REQUIREMENTS

This section provides requirements that differ from or are required in addition to those published in the CIS RHEL 5 Benchmark. These differences include amendments to settings in the CIS Benchmark and additional requirements identified through review of the Defense Information Systems Agency (DISA) RHEL 5 Security Technical Implementation Guide (STIG).

3.1 Requirements that are Different from the CIS Benchmark

This section provides the NRC-specific requirements that are different from the published CIS Benchmark requirements. In Table 3.1-1 below, the section headers match the headers in the CIS Benchmark; DISA requirements were added to the appropriate sections.

The following defines the information contained within the columns of Table 3.1-1:

- Step: The unique identifier of this configuration item within this standard.
- Source: The identification of the source (e.g., CIS, DISA) for the requirement.
- CIS/DISA ID: The CIS/DISA identifier number for this configuration item. Some items have multiple IDs, which indicate that different attributes of multiple requirements from an external standard were combined into a single requirement for this standard.
- Setting Name: The configuration item or issue.
- CIS/DISA Setting: The configuration setting per the CIS Benchmark or DISA STIG.
- NRC-Specific Requirement: The NRC setting (which is different from the CIS Benchmark requirement) for a configuration item.
- Rationale: This field provides the rationale for the NRC-specific requirement that is different from the published setting in the CIS Benchmark.

Table 3.1-1: RHEL 5 NRC-Specific Requirements that are Different from the CIS Benchmark

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
1.4 Advanced Intrusion Detection Environment (AIDE)						
1.	CIS	CIS-RHEL5: 1.4.2	Implement Periodic Execution of File Integrity	Set file checking on a periodic basis to determine if critical files have been changed in an unauthorized fashion. The suggested setting in the benchmark is daily.	NRC standards provide the minimum frequency required for conducting file integrity checks.	CSO-STD-0020, “Organization Defined Values for System Security Controls Standard” (SI-7 (1)), establishes the minimum frequency required for conducting file integrity checks.
1.7 Additional Process Hardening						
2.	DISA	GEN001780	Global initialization file configuration - "mesg -n" or "mesg n"	Global initialization files must contain the "mesg -n" or "mesg n" commands.	NRC requires the DISA STIG’s setting for the global initialization files containing the "mesg -n" or "mesg n" commands.	If the "mesg -n" or "mesg n" command is not placed into the system profile, messaging can be used to cause a Denial of Service attack.
3. Special Purpose Services						
3.	CIS	CIS-RHEL5: 3.2	Remove X Windows	Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.	Remove X Windows unless explicitly authorized by the system ISSO. Please note that there are additional hardening requirements that apply to the use of X Windows if use is authorized by the system ISSO. These requirements are provided in the CIS Benchmark and are included in this table (e.g., the requirements for X Windows file permissions in this section).	If there is a business need, the system ISSO can authorize specific servers to run X Windows. The authorization and rationale supporting the need to run X Windows on specific server(s) must be documented.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
4.	CIS	CIS-RHEL5: 3.6	Configure NTP	Configure Network Time Protocol (NTP) to ensure that clocks are synchronized across systems.	NRC standards require systems and network devices to synchronize a system's clock with the NRC time source or a time server appropriate to another agency-owned network. To enable correlation of events for audit logs, all systems must reference the same time source.	CSO-STD-2005, "NRC System Monitoring Standard," establishes the NRC requirement for the specific time servers to be used. CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AU-8 (1)), establishes time synchronization requirements.
5.	DISA	GEN000242	Number of clock synchronization sources	The system must use at least two time sources for clock synchronization.	NRC requires the DISA STIG's setting for the number of clock synchronization sources.	A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. For redundancy, two time sources are required so synchronization continues to function if one source fails. If the system is completely isolated (i.e., it has no connections to networks or other systems), time synchronization is not required as no correlation of events or operation of time-dependent protocols between systems will be necessary. If the system is completely isolated, this requirement is not applicable.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
6.	DISA	GEN005160	Writing .Xauthority files	Any X Windows host must write .Xauthority files.	NRC requires the DISA STIG's setting for .Xauthority files.	.Xauthority files ensure the user is authorized to access a specific X Windows host. If .Xauthority files are not used, it may be possible to obtain unauthorized access to the X Windows host.
7.	DISA	GEN005220	Use of .Xauthority files	.Xauthority or X*.hosts (or equivalent) file(s) must be used to restrict access to the X server.	NRC requires the DISA STIG's setting for .Xauthority files.	If access to the X server is not restricted, a user's X session may be compromised.
8.	DISA	GEN005240	Access to authorized hosts by the .Xauthority utility	The .Xauthority utility must only permit access to authorized hosts.	NRC requires the DISA STIG's setting for .Xauthority files.	If unauthorized clients are permitted access to the X server, a user's X session may be compromised.
9.	DISA	GEN005180, GEN005190	.Xauthority file configuration	All .Xauthority files must have mode 0600 or less permissive and must not have extended access control lists (ACLs).	NRC requires the DISA STIG's setting for the .Xauthority file configuration.	.Xauthority files ensure the user is authorized to access a specific X Windows host. Excessive permissions may permit unauthorized modification of these files, which could lead to Denial of Service to authorized access or allow unauthorized access to be obtained.
10.	DISA	GEN005200	X display exporting	X displays must not be exported to the world.	NRC requires the DISA STIG's setting for the X display exporting.	Open X displays allow an attacker to capture keystrokes and to execute commands remotely. Many users have their X Server set to "xhost +", permitting access to the X Server by anyone, from anywhere.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
11.	DISA	GEN000000-LNX00380	X server options configuration	An X server must not have the following options enabled: -ac, -core (except for debugging purposes), or -nolock.	NRC requires the DISA STIG's setting for the X server options configuration.	These options will detract from the security of the X Windows system by preventing a server from automatically being locked when the X screensaver is invoked, disabling access control restrictions, and resulting in the generation of core dumps.
12.	DISA	GEN005760	NFS export configuration file	The Network File System (NFS) export configuration file must have mode 0644 or less permissive.	NRC requires the DISA STIG's setting for the NFS export configuration file.	Excessive permissions on the NFS export configuration file could allow unauthorized modification of the file, which could result in Denial of Service to authorized NFS exports and the creation of additional unauthorized exports.
5. Logging and Auditing						
13.	CIS	CIS-RHEL5: 5.2.3	Configure /etc/rsyslog.conf	Configure rsyslog instead of syslog because of syslog inherent limitations (e.g., lack of authentication for client and server, lack of encryption, or reliable network transport).	NRC standards establish specific requirements for the information that must be recorded and retained in logs.	The specific NRC requirements for auditing and logging can be found in CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AU-2 and AU-3). CSO-STD-2005, "NRC System Monitoring Standard," also establishes NRC requirements for auditing.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
14.	CIS	CIS-RHEL5: 5.3.2.2	Disable System on Audit Log Full	The auditd daemon can be configured to halt the system when the audit logs are full. The benchmark recommends this configuration setting in high security contexts based on the assumption that the unavailability of the system is preferable to not detecting unauthorized access or nonrepudiation.	NRC standards provide the required actions to perform when audit logs are full.	CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AU-5), establishes the required actions to perform when audit logs are full.
6. System Access, Authentication and Authorization						
15.	CIS	CIS-RHEL5: 6.2.5	Set SSH MaxAuthTries to 4 or Less.	Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the Secure Shell (SSH) server. Set the maximum number of access attempts within a 15 minute time interval. The benchmark recommends setting this to 4.	NRC standards establish limits for the number of consecutive invalid access attempts by a user based on the security categorization of the system, whether the password is for an administrator, and the level of protection required for the information on the system.	CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AC-7), establishes the maximum number of consecutive invalid access attempts.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
16.	CIS	CIS-RHEL5: 6.2.14	Set SSH Banner	Set the Banner parameter. This banner is used to warn connecting users of an organization's appropriate use standards and requirements.	NRC standards require that systems be configured to display warning banners to users when they initially access an NRC IT system.	CSO-GUID-1102, "NRC Password and Warning Banner Guidance," establishes the NRC standard for warning banners.
7. User Accounts and Environment						
17.	CIS	CIS-RHEL5: 6.3.1	Set Strong Password Creation Policy using pam_cracklib	Set the values in pam_cracklib.so to check the strength of passwords.	NRC standards establish criteria for passwords based on the security categorization of the system, whether the password is for an administrator, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the minimum length for user passwords depending on the criticality of the system and whether the user is an administrator.
18.	CIS	CIS-RHEL5: 6.3.2	Set Strong Password Creation Policy Using pam_passwdqc	The pam_passwdqc.so module checks for password strength. Set the password strength by setting the number of character classes and password length.	NRC standards establish criteria for passwords based on the security categorization of the system, whether the password is for an administrator, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the minimum number of characters in a password depending on the criticality of the system and whether the password is for an administrator.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
19.	CIS	CIS-RHEL5: 6.3.3	Set Lockout for Failed Password Attempts	Set the number of failed password attempts before the account is locked. Changes need to be made to the main Pluggable Authentication Module (PAM) configuration file and also to the program specific PAM configuration file (e.g., Security Shell [SSH]).	NRC standards establish limits for the number of consecutive invalid access attempts by a user based on the security categorization of the system, whether the password is for an administrator, and the level of protection required for the information on the system.	CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AC-7), establishes the maximum number of consecutive invalid access attempts.
20.	CIS	CIS-RHEL5: 6.3.6	Limit Password Reuse	The /etc/security/opasswd file stores the user's old passwords and can be checked to ensure that users are not recycling recent passwords. The default setting is the last 5 passwords.	NRC standards establish criteria for passwords based on the security categorization of the system, whether the password is for an administrator, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the number of generations of passwords required dependent on system sensitivity level or whether the user is a system administrator.
21.	CIS	CIS RHEL5: 7.2.2	Set Password Change Minimum Number of Days	The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last change. The benchmark recommends preventing a user from changing a password for a minimum of 7 days.	NRC standards establish criteria for password strength based on the security categorization of the system, whether the password is for an administrator, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard" establishes the number of generations of passwords required dependent on system sensitivity level or whether the user is a system administrator.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
22.	DISA	GEN001845	Global initialization files' library search paths	Global initialization files' library search paths must contain only absolute paths.	NRC requires the DISA STIG's setting for the global initialization files' library search paths.	The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.
23.	DISA	GEN001850	Global initialization files' preloaded libraries	Global initialization files' lists of preloaded libraries must contain only absolute paths.	NRC requires the DISA STIG's setting for the global initialization files' preloaded libraries.	The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with a slash (/) are absolute paths.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
24.	DISA	GEN001901	Local initialization files' library search paths	Local initialization files' library search paths must contain only absolute paths.	NRC requires the DISA STIG's setting for the local initialization files' library search paths.	The library search path environment variable(s) contain a list of directories for the dynamic linker to search to find libraries. If this path includes the current working directory or other relative paths, libraries in these directories may be loaded instead of system libraries. This variable is formatted as a colon-separated list of directories. If there is an empty entry, such as a leading or trailing colon, or two consecutive colons, this is interpreted as the current working directory. Paths starting with a slash (/) are absolute paths.
25.	DISA	GEN001902	Local initialization files' preloaded libraries	Local initialization files' lists of preloaded libraries must contain only absolute paths.	NRC requires the DISA STIG's setting for the local initialization files' preloaded libraries.	The library preload list environment variable contains a list of libraries for the dynamic linker to load before loading the libraries required by the binary. If this list contains paths to libraries relative to the current working directory, unintended libraries may be preloaded. This variable is formatted as a space-separated list of libraries. Paths starting with a slash (/) are absolute paths.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
26.	DISA	GEN002120	The /etc/shells (or equivalent) file configuration	The /etc/shells (or equivalent) file must exist.	NRC requires the DISA STIG's setting for the /etc/shells (or equivalent) file configuration.	The shells file (or equivalent) lists approved default shells. It helps provide layered defense to the security approach by ensuring users cannot change their default shell to an unauthorized unsecure shell.
27.	DISA	GEN002140	/etc/passwd list of shells	All shells referenced in /etc/passwd must be listed in the /etc/shells file, except any shells specified for the purpose of preventing logins.	NRC requires the DISA STIG's setting for the /etc/passwd list of shells.	The shells file lists approved default shells. It helps provide layered defense to the security approach by ensuring users cannot change their default shell to an unauthorized unsecure shell.
28.	DISA	GEN000000-LNX00580	CTRL-ALT-DELETE key sequence	The x86 CTRL-ALT-DELETE key sequence must be disabled.	NRC requires the DISA STIG's setting for the CTRL-ALT-DELETE key sequence.	Undesirable reboots can occur if the CTRL-ALT-DELETE key sequence is not disabled. Such reboots may cause a loss of data or loss of access to critical information.
8. Warning Banners						
29.	CIS	CIS RHEL5: 8.1	Set Warning Banner for Standard Login Services	Set the warning banner of standard login. This benchmark establishes the requirement that the contents of /etc/issue are displayed prior to the login prompt both on the system console and serial devices as well as prior to logins via Telnet.	NRC standards require that systems shall be configured to display warning banners to users when they initially access an NRC IT system.	CSO-GUID-1102, "NRC Password and Warning Banner Guidance," establishes the NRC requirements for warning banners.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
30.	CIS	CIS RHEL5: 8.2	Set GNOME Warning Banner	Edit the file /user/share/gdm/themes/ RHEK/RHEL.xml. Set the warning banner displayed for GNOME users before they log in warning them of their legal status regarding the system and monitoring policies that are in place.	NRC standards require that systems shall be configured to display warning banners to users when they initially access an NRC IT system.	CSO-GUID-1102, "NRC Password and Warning Banner Guidance," establishes the NRC standards require for warning banners.
9.1 Verify System File Permissions						
31.	DISA	GEN000000-LNX00400, GEN000000-LNX00420, GEN000000-LNX00440, GEN000000-LNX00450	/etc/security/access.conf file configuration	The /etc/security/access.conf file must be owned by root, must have a privileged group owner, must have mode 0640 or less permissive, and must not have an extended access control list (ACL).	NRC requires the DISA STIG's setting for the /etc/security/access.conf file configuration.	The /etc/security/access.conf file contains entries restricting access from the system console by authorized System Administrators. If the file is owned by a user other than root, it could compromise the system. If the group owner were not a privileged group, it could endanger system security. If the access permissions are more permissive than 0640, system security could be compromised.
32.	DISA	GEN000000-LNX00480, GEN000000-LNX00500, GEN000000-LNX00520, GEN000000-LNX00530	/etc/sysctl.conf file configuration	The /etc/sysctl.conf file must be owned by root, must be group-owned by root, must have mode 0600 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/sysctl.conf file configuration.	The sysctl.conf file specifies the values for kernel parameters to be set on boot. These settings can affect the system's security.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
33.	DISA	GEN000000-LNX00620, GEN000000-LNX00640, GEN000000-LNX00660	/etc/securetty file configuration	The /etc/securetty file must be group-owned by root, sys, or bin, must be owned by root, and must have mode 0640 or less permissive.	NRC requires the DISA STIG's setting for the /etc/securetty file configuration.	The securetty file contains the list of terminals permitting direct root logins. It must be protected from unauthorized modification.
34.	DISA	GEN001362, GEN001363, GEN001364, GEN001365	/etc/resolv.conf file configuration	The /etc/resolv.conf file must be owned by root, must be group-owned by root, bin, or sys, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/resolv.conf file configuration.	The resolv.conf (or equivalent) file configures the system's Domain Name System (DNS) resolver. DNS is used to resolve host names to IP addresses. If DNS configuration is modified maliciously, host name resolution may fail or return incorrect information. DNS may be used by a variety of system security functions such as time synchronization, centralized authentication, and remote system logging.
35.	DISA	GEN001366, GEN001367, GEN001368, GEN001369	/etc/hosts file configuration	The /etc/hosts file must be owned by root, must be group-owned by root, bin, or sys, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/hosts file configuration.	The /etc/hosts file (or equivalent) configures local host name to Internet Protocol (IP) address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, it could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
36.	DISA	GEN001371, GEN001372, GEN001373, GEN001374	/etc/nsswitch.conf file configuration	The /etc/nsswitch.conf file must be owned by root, must be group-owned by root, bin, or sys, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/nsswitch.conf file configuration.	The nsswitch.conf file (or equivalent) configures the source of a variety of system security information including account, group, and host lookups. Malicious changes could prevent the system from functioning or compromise system security.
37.	DISA	GEN001720, GEN001730, GEN001740, GEN001760	Global initialization file configuration /etc/bashrc, /etc/csh.cshrc, /etc/csh.login, /etc/csh.logout, /etc/environment, /etc/ksh.kshrc, /etc/profile, /etc/suid_profile, /etc/profile.d/*	All global initialization files must have mode 0644 or less permissive, must not have extended ACLs, must be owned by root, and must be group-owned by root, sys, bin, other, system, or the system default.	NRC requires the DISA STIG's setting for the global initialization file configuration.	Global initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.
38.	DISA	GEN001800, GEN001810, GEN001820, GEN001830	Skeleton file configuration	All skeleton files (typically those in /etc/skel) must have mode 0644 or less permissive, must not have extended ACLs, must be owned by root or bin, and must be group-owned by root, bin, sys, system, or other.	NRC requires the DISA STIG's setting for the skeleton file configuration.	If the skeleton files are not protected, unauthorized personnel could change user startup parameters and possibly jeopardize user files.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
39.	DISA	GEN001860, GEN001870, GEN001880, GEN001890	Local initialization file configuration	All local initialization files must be owned by the home directory's user or root, must be group-owned by the user's primary group or root, must have mode 0740 or less permissive, and must not have extended ACLs.	NRC requires the DISA STIG's setting for the local initialization file configuration.	Local initialization files are used to configure the user's shell environment upon login. Malicious modification of these files could compromise accounts upon logon.
40.	DISA	GEN002200, GEN002210, GEN002220, GEN002230	Shell file configuration	If shell files are owned by users other than root or bin, they could be modified by intruders or malicious users to perform unauthorized actions.	NRC requires the DISA STIG's setting for the shell file configuration.	All shell files must be owned by root or bin, must be group-owned by root, bin, sys, or system, must have mode 0755 or less permissive, and must not have extended ACLs.
41.	DISA	GEN003730, GEN003740, GEN003745, GEN003750	The inetd.conf file, xinetd.conf file, and the xinetd.d directory configurations	The inetd.conf file, xinetd.conf file, and the xinetd.d directory must be group-owned by root, bin, sys, or system. The inetd.conf and xinetd.conf files must have mode 0440 or less permissive and must not have extended ACLs. The xinetd.d directory must have mode 0755 or less permissive.	NRC requires the DISA STIG's setting for the inetd.conf file, xinetd.conf file, and the xinetd.d directory configurations,	Failure to configure ownership and permissions of sensitive files or utilities to system groups may provide unauthorized users with the potential to access sensitive information or change the system configuration possibly weakening the system's security posture.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
42.	DISA	GEN003760, GEN003770, GEN003780, GEN003790	services file configuration	The services file must be owned by root or bin, must be group-owned by root, bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the services file configuration.	Failure to give ownership of sensitive files or utilities to root or bin provides the designated owner and unauthorized users with the potential to access sensitive information or change the system configuration possibly weakening the system's security posture.
43.	DISA	GEN004480, GEN004500, GEN004510	SMTP service log file configuration	The Simple Mail Transport Protocol (SMTP) service log file must be owned by root, must have mode 0644 or less permissive and must not have an extended ACL.	NRC requires the DISA STIG's setting for the SMTP service log file configuration.	If the SMTP service log file is not owned by root, then unauthorized personnel may modify or delete the file to hide a system compromise.
44.	DISA	GEN005740, GEN005750, GEN005760, GEN005770	NFS export configuration file	The NFS export configuration file must be owned by root, must be group-owned by root, bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the NFS export configuration file.	Failure to configure the NFS export configuration file to root provides the designated owner and possible unauthorized users with the potential to change system configuration which could weaken the system's security posture.
45.	DISA	GEN006100, GEN006120, GEN006140, GEN006150	/etc/smb.conf file configuration	The /etc/smb.conf file must be owned by root, must be group-owned by root, bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/smb.conf file configuration.	The /etc/smb.conf file allows access to other machines on the network and grants permissions to certain users. If it is owned by another user, the file may be maliciously modified and the Samba configuration could be compromised.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
46.	DISA	GEN006160, GEN006180, GEN006200, GEN006210	/etc/smbpasswd file configuration	The /etc/smbpasswd file must be owned by root, must be group-owned by root, must have mode 0600 or less permissive and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/smbpasswd file configuration.	If the "smbpasswd" file is not owned by root, it may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.
47.	DISA	GEN008060, GEN008080, GEN008100, GEN008120	/etc/ldap.conf (or equivalent) file configuration	If the system is using Lightweight Directory Access Protocol (LDAP) for authentication or account information the /etc/ldap.conf (or equivalent) file must have mode 0644 or less permissive, must be owned by root, must be group-owned by root, bin, sys, or system, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the /etc/ldap.conf (or equivalent) file configuration.	LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.
48.	DISA	GEN008140, GEN008160, GEN008180, GEN008200	TLS certificate authority file and/or directory configuration	If the system is using LDAP for authentication or account information, the Transport Layer Security (TLS) certificate authority file and/or directory (as appropriate) must be owned by root, must be group-owned by root, bin, sys, or system, must have mode 0644 (0755 for directories) or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the TLS certificate authority file and/or directory configuration.	LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
49.	DISA	GEN008220, GEN008240, GEN008260, GEN008280	TLS certificate file configuration	For systems using Name Service Switch (NSS) LDAP, the TLS certificate file must be owned by root, must be group-owned by root, bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the TLS certificate file configuration.	The NSS LDAP service provides user mappings which are a vital component of system security. Its configuration must be protected from unauthorized modification.
50.	DISA	GEN008300, GEN008320, GEN008340, GEN008360	LDAP TLS key file configuration	If the system is using LDAP for authentication or account information, the LDAP TLS key file must be owned by root, must be group-owned by root, bin, or sys, must have mode 0600 or less permissive, and must not have an extended ACL.	NRC requires the DISA STIG's setting for the LDAP TLS key file configuration.	LDAP can be used to provide user authentication and account information, which are vital to system security. The LDAP client configuration must be protected from unauthorized modification.
51.	DISA	GEN002680, GEN002690, GEN002700, GEN002710	System audit log file configurations	System audit logs must be owned by root, must be group-owned by root, bin, sys, or system, must have mode 0640 or less permissive and must not have extended ACLs.	NRC requires the DISA STIG's setting for the system audit log file configurations.	Sensitive system and user information could provide a malicious user with enough information to penetrate further into the system.
52.	DISA	GEN002715, GEN002716, GEN002717, GEN002718	System audit tool executable configuration	System audit tool executables must be owned by root, must be group-owned by root, bin, sys, or system, must have mode 0750 or less permissive, and must not have extended ACLs.	NRC requires the DISA STIG's setting for the system audit tool executable configuration.	To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.

This page intentionally left blank.

4 DEFINITIONS

External Standard	An external security standard (e.g., a configuration baseline or set of requirements for the use of a technology or technologies) developed by a U.S. Government agency (e.g., Committee on National Security Systems [CNSS], DISA, National Security Agency [NSA], National Institute of Standards and Technology [NIST]), private organization (e.g., CIS), or a software / hardware vendor. External standards are used by the NRC as the basis for NRC cyber security standards.
GNOME	A desktop environment and graphical user interface that runs on top of a computer operating system, most notably Linux.

This page intentionally left blank.

5 ACRONYMS

ACL	Access Control List
AIDE	Advanced Intrusion Detection Environment
ATO	Approval to Operate
CIS	Center for Internet Security
CNSS	Committee on National Security Systems
CSO	Computer Security Office
DAA	Designated Approving Authority
DISA	Defense Information Systems Agency
DNS	Domain Name System
DR	Deviation Request
IP	Internet Protocol
ISSO	Information System Security Officer
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSS	Name Service Switch
NTP	Network Time Protocol

PAM	Pluggable Authentication Module
RHEL	Red Hat Enterprise Linux
SGI	Safeguards Information
SMB	Server Message Block
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell
STD	Standard
STIG	Security Technical Implementation Guide
SUNSI	Sensitive Unclassified Non-Safeguards Information
TLS	Transport Layer Security
TTY	Teletypewriter
UID	User Identifier
XML	Extensible Markup Language

CSO-STD-1418 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
26-Jun-13	1.0	Initial issuance	Distribution at ISSO forum and posting on CSO web page	Upon request