

Nuclear Regulatory Commission
 Computer Security Office
 Computer Security Standard

Office Instruction: **CSO-STD-1417**

Office Instruction Title: **IBM AIX 6.1 Server Configuration Standard**

Revision Number: **1.0**

Effective Date: **January 1, 2014**

Primary Contacts: **Kathy Lyons-Burke, SITSO**

Responsible Organization: **CSO/PST**

Summary of Changes: CSO-STD-1417, "IBM AIX 6.1 Server Configuration Standard" provides the minimum configuration settings that must be applied to NRC servers running AIX 6.1 operating systems.

Training: As requested

ADAMS Accession No.: **ML13255A205**

Approvals				
Primary Office Owner	Policies, Standards, and Training		Signature	Date
Standards Working Group Chair	Bill Dabbs		/RA/	10/9/13
Responsible SITSO	Kathy Lyons-Burke		/RA/	10/9/13
DAA for Non-Major IT Investments	Director, CSO	Tom Rich	/RA/	10/9/13
	Director, OIS	Jim Flanagan	/RA/	10/9/13

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 27

5 ACRONYMS 29

Computer Security Standard CSO-STD-1417

IBM AIX 6.1 Server Configuration Standard

1 PURPOSE

CSO-STD-1417, “IBM® AIX® 6.1 Server Configuration Standard,” provides configuration settings for the Nuclear Regulatory Commission (NRC) servers running the IBM Advanced Interactive eXecutive (AIX) 6.1 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 AIX 6.1 operating systems. AIX 6.1 servers must meet all federally mandated and NRC-defined security requirements.

2 GENERAL REQUIREMENTS

All NRC servers running the AIX 6.1 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.

AIX 6.1 servers operated by the NRC or other parties on behalf of the NRC must comply with the Center for Internet Security (CIS) AIX 6.1 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 IBM and AIX are registered trademarks of the International Business Machines (IBM) Corporation.

3 SPECIFIC REQUIREMENTS

This section provides requirements that differ from or are required in addition to those published in the CIS AIX 6.1 Benchmark. These differences include amendments to settings in the CIS Benchmark and additional requirements identified through a review of the Defense Information Systems Agency (DISA) AIX 6.1 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 3.1.1-1: AIX 6.1 NRC-Specific Requirements that are Different from the CIS Benchmark

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
1.1 AIX Security Expert – Password Policy						
1.	CIS	CIS-AIX 5.3-6.1: 1.1.1	/etc/security/user – mindiff	In /etc/security/user, set the default mindiff attribute to be greater than or equal to 4 for the minimum number of characters that are required in a new password which were not in the old password.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.
2.	CIS	CIS-AIX 5.3-6.1: 1.1.2	/etc/security/user – minage	In /etc/security/user, set the default minage attribute to 1 for the minimum number of weeks before a password can be changed.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.
3.	CIS	CIS-AIX 5.3-6.1: 1.1.3	/etc/security/user – maxage	In /etc/security/user, set the default maxage attribute to be less than or equal to 13 for the maximum number of weeks that a password is valid.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
4.	CIS	CIS-AIX 5.3-6.1: 1.1.4	/etc/security/user - minlen	In /etc/security/user, set the default minlen attribute to be greater than or equal to 8 for the minimum length of a password.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.
5.	CIS	CIS-AIX 5.3-6.1: 1.1.5	/etc/security/user - minalpha	In /etc/security/user, set the default minalpha attribute to be greater than or equal to 2 for the minimum number of alphabetic characters in a password.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.
6.	CIS	CIS-AIX 5.3-6.1: 1.1.6	/etc/security/user - minother	In /etc/security/user, set the default minother attribute to be greater than or equal to 2 for the number of characters within a password that must be non-alphabetic.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirement for these values.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
7.	CIS	CIS-AIX 5.3-6.1: 1.1.9	/etc/security/user - histsize	In /etc/security/user, set the default histsize attribute to be greater than or equal to 20 for the number of previous passwords to be stored in the password history to prevent password reuse.	NRC establishes password requirements based on the security categorization of the system, whether the password is an administrative password, and the level of protection required for the information on the system.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.
8.	CIS	CIS-AIX 5.3-6.1: 1.1.11	/etc/security/login .cfg – pwd_algorithm	In /etc/security/login.cfg, set the user stanza pwd_algorithm attribute to sha256. CIS recommends setting the password algorithm to sha256 to support long passwords.	Encryption must be implemented according to the requirements in CSO-STD-2009, "Cryptographic Control Standard."	CSO-STD-2009, "Cryptographic Control Standard" provides the NRC requirements for cryptography.
1.2 AIX Security Expert – Login Policy						
9.	CIS	CIS-AIX 5.3-6.1: 1.2.6	/etc/security/user – loginretries	In /etc/security/user, set the default loginretries attribute to 3 for the number of invalid login attempts prior to the user account being locked automatically.	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
1.3 AIX Security Expert – System Services Management						
10.	CIS	CIS-AIX 5.3-6.1: 1.3.31	/etc/inetd.conf – time	In /etc/inetd.conf, comment out the time entries. The synchronization of time service is obsolete and has been superseded by Network Time Protocol (NTP).	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 requirements 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.
11.	DISA	GEN000250, GEN000251, GEN000252, GEN000253	Time synchronization configuration file (/etc/ntp.conf)	The time synchronization configuration file (such as /etc/ntp.conf) must be owned by root, must be group-owned by bin, sys, or system, must have mode 0640 or less permissive and must not have an extended Access Control List (ACL).	NRC adheres to the DISA STIG's setting for the time synchronization configuration file.	A synchronized system clock is critical for the enforcement of time-based policies and the correlation of logs and audit records with other systems. If an illicit time source is used for synchronization, the integrity of system logs and the security of the system could be compromised. If the configuration files controlling time synchronization are not protected, unauthorized modifications could result in the failure of time synchronization.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
12.	DISA	GEN000242	Number of clock synchronization sources	The system must use at least two time sources for clock synchronization.	NRC adheres to the DISA STIG's setting for the number of clock synchronization sources if a system connects to networks or other systems. If a system is completely isolated, time synchronization (and two time sources) is not required.	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 (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.
13.	CIS	CIS-AIX 5.3-6.1: 1.3.35	/etc.inetd.conf – ftp	In /etc/inetd.conf, comment out the ftp entry. File Transfer Protocol (FTP) should not be started automatically. FTP is an unencrypted network protocol; FTP should only be used if there is a mission critical reason to do so.	NRC standards restrict the use of FTP.	CSO-STD-2008, "NRC Network Protocol Standard," specifically restricts the use of FTP at NRC.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
14.	DISA	GEN000000-AIX0300	bootp service disabled	The system must not have the bootp service active.	NRC adheres to the DISA STIG's setting for disabling the bootp service.	The bootp service is used for Network Installation Management (NIM) and remote booting of systems. The bootp service should not be active unless it is needed for NIM servers or booting remote systems. Running unnecessary services increases the attack vector of the system.
1.6 AIX Security Expert – TCP/IP Hardening						
15.	DISA	GEN000000-AIX0210	tcp_icmpsecure	The system must provide protection from Internet Control Message Protocol (ICMP) attacks on Transmission Control Protocol (TCP) connections.	NRC adheres to the DISA STIG's setting for tcp_icmpsecure.	The ICMP attacks may be in the form of ICMP source quench attacks and Path Maximum Transmission Unit Discovery (PMTUD) attacks. If this network option tcp_icmpsecure is turned on, the system does not react to ICMP source quench messages. This will protect against ICMP source quench attacks. The payload of the ICMP message is tested to determine if the sequence number of the TCP header portion of the payload is within the range of acceptable sequence numbers. This will mitigate PMTUD attacks to a large extent.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
16.	DISA	GEN007820	IP tunnel configuration	The system must not have Internet Protocol (IP) tunnels configured.	NRC adheres to the DISA STIG's setting for IP tunnel configuration.	IP tunneling mechanisms can be used to bypass network filtering.
17.	DISA	GEN007900	Reverse-path filter for IPv6 network traffic	The system must use an appropriate reverse-path filter for IPv6 network traffic, if the system uses IPv6.	NRC adheres to the DISA STIG's setting for reverse-path filters for IPv6 network traffic.	Reverse-path filtering provides protection against spoofed source addresses by causing the system to discard packets that have source addresses for which the system has no route or if the route does not point towards the interface on which the packet arrived. Depending on the role of the system, reverse-path filtering may cause legitimate traffic to be discarded; therefore, should be used with a more permissive mode or filter, or not at all. Whenever possible, reverse-path filtering should be used.
18.	DISA	GEN007780	Disable 6to4	The system must not have 6to4 enabled.	NRC adheres to the DISA STIG's setting for disabling 6to4.	6to4 is an IPv6 transition mechanism that involves tunneling IPv6 packets encapsulated in IPv4 packets on an ad-hoc basis. This is not a preferred transition strategy and increases the attack surface of the system.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
19.	DISA	GEN000000-AIX0230	IP fragmentation attacks protection	The system must provide protection against IP fragmentation attacks.	NRC adheres to the DISA STIG's setting for IP fragmentation attacks protection.	The parameter ip_nfrag provides an additional layer of protection against IP fragmentation attacks. The value the ip_nfrag specifies is the maximum number of fragments of an IP packet that can be kept in the IP reassembly queue at any time. The default value of this network option is 200. This is a reasonable value for most environments and offers protection from IP fragmentation attacks.
20.	DISA	GEN003602	ICMP timestamp requests	The system must not process ICMP timestamp requests.	NRC adheres to the DISA STIG's setting for ICMP timestamp requests.	Processing ICMP timestamp requests increases the attack surface of the system.
21.	DISA	GEN003611	Martian packets	The system must log martian packets. Add rules to log inbound traffic containing invalid source addresses, which minimally include the system's own addresses and broadcast addresses for attached subnets.	NRC adheres to the DISA STIG's setting for logging martian packets.	Martian packets are packets containing addresses known by the system to be invalid. Logging the receipt of these packets allows the system administrator to identify misconfigurations or attacks in progress.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
1.7 AIX Security Expert – Miscellaneous Enhancements						
22.	CIS	CIS-AIX 5.3-6.1: 1.7.7	Miscellaneous Enhancements – default umask	<p>Check global initialization files for the configured umask value.</p> <p>Check local initialization files for the configured umask value.</p> <p>The system and user default umask must be 077.</p>	NRC adheres to the DISA STIG's setting for default umask.	The umask controls the default access mode assigned to newly created files. An umask of 077 limits new files to mode 700 or less permissive. Although umask can be represented as a 4-digit number, the first digit representing special access modes is typically ignored or required to be 0. This requirement applies to the globally configured system defaults and the user defaults for each account on the system.
23.	DISA	GEN002715, GEN002716, GEN002717, GEN002718	System audit tool executables	<p>System audit tool executables (e.g., audit, auditcat, auditconv, auditpr, auditselect, auditstream, auditbin, and auditmerge) must be owned by root, must be group-owned by bin, sys, or system, must have mode 0750 or less permissive, and must not have extended ACLs.</p>	NRC adheres to the DISA STIG's setting for system audit tool executables.	To prevent unauthorized access or manipulation of system audit logs, the tools for manipulating those logs must be protected.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
24.	DISA	GEN006565	Periodic verification of system software	The system package management tool must be used to verify system software periodically. Check the root crontab for a job invoking the system package management tool to verify the integrity of installed packages.	NRC adheres to the DISA STIG's setting for periodic verification of system software.	The system package management tool can be used to verify that system software has not been tampered with.
25.	DISA	GEN006570	Verification of ACLs.	The file integrity tool must be configured to verify ACLs.	NRC adheres to the DISA STIG's setting for periodic verification of ACLs.	ACLs can provide permissions beyond those permitted through the file mode; therefore, they must be verified by file integrity tools.
26.	DISA	GEN006571	Verification of extended attributes	The file integrity tool must be configured to verify extended attributes.	NRC adheres to the DISA STIG's setting for periodic verification of extended attributes.	Extended attributes in file systems may contain arbitrary data and file metadata with security implications.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
2.1 Non AIX Security Expert Managed Recommendations – Configuring syslog						
27.	CIS	CIS-AIX 5.3-6.1: 2.1.1	Configuring Syslog – local logging	The benchmark recommends implementing a local syslog configuration which is not automatically established. The benchmark also recommends a weekly rotation in a four week cycle.	NRC standards establish specific requirements for the information that shall be recorded and retained in logs. NRC standards also establish the required frequency for Information System Security Officer (ISSO) log reviews based on the security categorization of the system and the information that must be retained from the audit log review.	CSO-STD-2005, "NRC System Monitoring Standard," establishes the NRC requirements for local logging. CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AU-2), establishes the events that shall be audited.
28.	CIS	CIS-AIX 5.3-6.1: 2.1.2	Configuring Syslog – remote logging	Explicitly define a remote host for auth.info data in /etc/syslog.conf. To further enhance the local syslog logging process, CIS recommends that syslog information, in particular that generated by the auth facility, is logged remotely.	NRC standards establish specific requirements for the information that shall be recorded and retained in logs.	CSO-STD-2005, "NRC System Monitoring Standard," establishes the NRC requirements for remote audit logging. CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AU-2), establishes the events that shall be audited.
29.	DISA	GEN005390, GEN005395, GEN005400, GEN005420	The syslog.conf file configuration	The /etc/syslog.conf file must be owned by root, must be group-owned by bin, sys, or system, must have mode 0640 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for syslog.conf file configuration.	Unauthorized users must not be allowed to access or modify the /etc/syslog.conf file.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
2.2 Non AIX Security Expert Managed Recommendations – Secure Remote Access						
30.	CIS	CIS-AIX 5.3-6.1: 2.2.5	Configuring SSH – banner configuration	<p>Edit the /etc/ssh/sshd_config file and configure a path to a login message.</p> <p>Set a login herald message that requires a user to accept the terms and conditions of an organization's acceptable usage standards.</p>	NRC standards establish the requirement that systems must 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 requirement for warning banners.
31.	DISA	GEN005521	SSH daemon login restrictions	The Secure Shell (SSH) daemon must restrict login ability to specific users and/or groups.	NRC adheres to the DISA STIG's setting for SSH daemon login restrictions.	Restricting SSH logins to a limited group of users, such as system administrators, prevents password-guessing, other SSH attacks from reaching system accounts, and other accounts not authorized for SSH access.
2.3 Non AIX Security Expert Managed Recommendations – Sendmail Configuration						
32.	DISA	GEN004480	SMTP service log file owner	<p>Identify any log files configured for the mail service at any severity level, or those configured for all services. Check the ownership of these log files.</p> <p>The Simple Mail Transport Protocol (SMTP) service log file must be owned by root.</p>	NRC adheres to the DISA STIG's setting for SMTP service log file owner.	NRC Standards and the CIS Benchmark do not provide a requirement for this setting. 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.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
33.	DISA	GEN004500	SMTP service log file permissions	Check the mode of the SMTP service log file. The SMTP service log file must have mode 0644 or less permissive.	NRC adheres to the DISA STIG's setting for SMTP service log file permissions.	NRC Standards and the CIS Benchmark do not provide a requirement for this setting. If the SMTP service log file is more permissive than 0644, unauthorized users may be allowed to change the log file.
34.	DISA	GEN004510	SMTP service log file extended ACL	Check if extended permissions are disabled. The SMTP service log file must not have an extended ACL.	NRC adheres to the DISA STIG's setting for SMTP service log file extended ACL permissions.	NRC Standards and the CIS Benchmark do not provide a requirement for this setting. If the SMTP service log file has an extended ACL, unauthorized users may be allowed to access or modify the log file.
2.4 Non AIX Security Expert Managed Recommendations – Common Desktop Environment (CDE)						
35.	CIS	CIS-AIX 5.3-6.1: 2.4.5	CDE – screensaver lock	Set the default timeout parameters dtsession*savertimeout: and dtsession*lockTimeout: Set a password protected screensaver invoked by the CDE session manager after 10 minutes of keyboard or mouse inactivity.	NRC standards establish specific requirements for the length of inactivity before initiating a session lock based on the categorization of the system.	CSO-STD-0020, "Organization Defined Values for System Security Controls Standard" (AC-11), establishes the length of inactivity before initiating a session lock.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
36.	DISA	GEN000510	Graphical desktop environment session lock pattern	The system must display a publicly-viewable pattern during a graphical desktop environment session lock.	NRC adheres to the DISA STIG's setting for the graphical desktop environment session lock pattern.	To protect the on-screen content of a session, the content must be replaced with a publicly-viewable pattern upon session lock. Examples of publicly viewable patterns include screen saver patterns, photographic images, solid colors, or a blank screen, so long as none of those patterns convey sensitive information.
37.	DISA	GEN005160	Any X Windows host must write .Xauthority files.	Check for .Xauthority files being utilized by looking for such files in the home directory of a user that uses X. Ensure the X Windows host is configured to write .Xauthority files into user home directories. Edit the Xaccess file. Ensure the line that writes the .Xauthority file is uncommented.	NRC adheres to the DISA STIG's setting for writing .Xauthority files.	.Xauthority files ensure the user is authorized to access the specific X Windows host. If .Xauthority files are not used, unauthorized access to the X Windows host may be obtained.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
38.	DISA	GEN005220	.Xauthority or X*.hosts (or equivalent) file(s) must be used to restrict access to the X server.	Search the system for an X*.hosts files, where * is a display number that may be used to limit X window connections. If no files are found, X*.hosts files are not being used. If the X*.hosts files contain any unauthorized hosts, this is a finding.	NRC adheres to the DISA STIG's setting for restricting access to the X server.	If access to the X server is not restricted, a user's X session may be compromised.
39.	DISA	GEN005240	The .Xauthority utility must only permit access to authorized hosts.	Remove unauthorized clients from the xauth configuration.	NRC adheres to the DISA STIG's setting for using the .Xauthority utility to only permit access to authorized hosts.	If unauthorized clients are permitted access to the X server, a user's X session may be compromised.
40.	DISA	GEN005200	X display exporting	X displays must not be exported to the world.	NRC adheres to the DISA STIG's setting for 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
41.	DISA	GEN005760, GEN005770	NFS export configuration file	The Network File System (NFS) export configuration file must have mode 0644 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for the NFS export configuration file.	File system extended ACLs provide access to files beyond what is allowed by the mode numbers of the files. 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.
2.5 Non AIX Security Expert Managed Recommendations – NFS						
42.	DISA	GEN005760	NFS export configuration file	The NFS export configuration file (chmod 0644 /etc/exports) must have mode 0644 or less permissive.	NRC adheres to the DISA STIG's setting for NFS export configuration file permissions.	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.
2.7 Non AIX Security Expert Managed Recommendations – SNMP						
43.	CIS	CIS-AIX 5.3-6.1: 2.7	SNMP	Define community strings that are greater than six characters and includes a combination of letters, numbers, and special characters.	With the System Network Monitoring Protocol (SNMP), community strings must be set using NRC standards that establish the requirements for strong passwords.	CSO-STD-0001, "NRC Strong Password Standard," establishes the NRC requirements for these values.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
44.	DISA	GEN005320, GEN005360, GEN005365, GEN005375	The snmpd.conf file configuration	The snmpd.conf file must have mode 0600 or less permissive, must be owned by root, must be group-owned by bin, sys, or system, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for snmpd.conf file configuration.	The snmpd.conf file contains authenticators and must be protected from unauthorized access and modification.
2.11 Non AIX Security Expert Managed Recommendations – Permissions and Ownership						
45.	DISA	GEN000000-AIX0085, GEN000000-AIX0090, GEN000000-AIX0100, GEN000000-AIX0110	The /etc/netd.conf file configuration	The /etc/netd.conf file must be root owned, must be group-owned by bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for using the /etc/netd.conf file configuration.	The /etc/netd.conf file is used to specify the ordering of name resolution for the sendmail command, alias resolution for the sendmail command, and host name resolution routines. Malicious changes could prevent the system from functioning correctly or compromise system security.
46.	DISA	GEN001362, GEN001363, GEN001364, GEN001365	The /etc/resolv.conf file configuration	The /etc/resolv.conf file must be root owned, must be group-owned by bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for using 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 the 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.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
47.	DISA	GEN001366, GEN001367, GEN001368, GEN001369	The /etc/hosts file configuration	The /etc/hosts file must be root owned, must be group-owned by bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for using the /etc/hosts file configuration.	The /etc/hosts file (or equivalent) configures local host name to IP address mappings that typically take precedence over DNS resolution. If this file is maliciously modified, the file could cause the failure or compromise of security functions requiring name resolution, which may include time synchronization, centralized authentication, and remote system logging.
48.	DISA	GEN001720, GEN001730, GEN001740, GEN001760	Global initialization file configuration	All global initialization files must be root owned, must be group-owned by bin, sys, security or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for 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.
49.	DISA	GEN001800, GEN001810, GEN001820, GEN001830	Skeleton file and directory configuration	All skeleton files and directories (typically in /etc/skel) must be owned by root or bin, must be group-owned by security, must have mode 0644 or less permissive, and must not have extended ACLs.	NRC adheres to the DISA STIG's setting for skeleton file and directory configurations.	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
50.	DISA	GEN001860, GEN001870, GEN001880, GEN001890	Local initialization file configuration	All local initialization files must be owned by the 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 adheres to the DISA STIG's setting for 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.
51.	DISA	GEN002200, GEN002210, GEN002220, GEN002230	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.	NRC adheres to the DISA STIG's setting for shell file configuration.	Shells with world/group write permissions give the ability to maliciously modify the shell to obtain unauthorized access. If shell files are group-owned by users other than root or a system group, they could be modified by intruders or malicious users to perform unauthorized actions. 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.
52.	DISA	GEN003760, GEN003770, GEN003780, GEN003790	The services file configuration	The services file must be owned by root or bin, must be group-owned by bin, sys, or system, must have mode 0444 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for services file configuration.	The services file is critical to the proper operation of network services and must be protected from unauthorized modification. Unauthorized modification could result in the failure of network services.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
53.	DISA	GEN006100, GEN006120, GEN006140, GEN006150	SMB configuration file	The /usr/lib/smb.conf file must be owned by root, must be group-owned by bin, sys, or system, must have mode 0644 or less permissive, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for the Server Message Block (SMB) configuration file.	A compromised configuration could endanger the security of the Samba configuration file and, ultimately, the system and network.
54.	DISA	GEN006210, GEN006200, GEN006180, GEN006160	smbpasswd file configuration	The /var/private/smbpasswd file must not have an extended ACL, must have mode 0600 or less permissive, must be group-owned by sys or system, and must be owned by root.	NRC adheres to the DISA STIG's setting for the smbpasswd file configuration.	If the smbpasswd file may be maliciously accessed or modified, potentially resulting in the compromise of Samba accounts.
55.	DISA	GEN008060, GEN008080, GEN008100, GEN008120	ldap.conf 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 security, bin, sys, or system, and must not have an extended ACL.	NRC adheres to the DISA STIG's setting for the ldap.conf 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.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
56.	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 Protocol (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 adheres to 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.
2.12 Non AIX Security Expert Managed Recommendations – Miscellaneous Configuration Changes						
57.	DISA	GEN003540	Non-Executable Program Stacks.	On 64-bit systems, verify the sed_config (Stack Execution Disable) setting is "all." (32-bit systems do not support sed_config. This is a permanent finding on 32-bit AIX systems.)	NRC adheres to the DISA STIG's setting for non-executable program stacks.	A common type of exploit is the stack buffer overflow. An application receives, from an attacker, more data than the application is prepared for and stores this information on its stack, writing beyond the reserved space. This can be designed to cause execution of the data written on the stack. One mechanism to mitigate this vulnerability is for the system to prohibit the execution of instructions in sections of memory identified as part of the stack.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
58.	CIS	CIS-AIX 5.3-6.1: 2.12.11	Miscellaneous Config – ftp banner	If FTP is required on the system, establish an FTP login banner that displays necessary warning to users trying to gain unauthorized access to the system and that all activity will be monitored and reported.	NRC standards restrict the use of FTP.	CSO-STD-2008, "NRC Network Protocol Standard," specifically restricts the use of FTP at NRC.
59.	CIS	CIS-AIX 5.3-6.1: 2.12.12	Miscellaneous Config – /etc/motd	Create a /etc/motd file. Set a post initial login statutory warning message that could aid in the prosecution of offenders guilty of unauthorized system access.	NRC standards establish the specific requirement that systems must 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.
60.	DISA	GEN000340	System account UID reservations	User Identifiers (UIDs) reserved for system accounts must not be assigned to non-system accounts.	NRC adheres to the DISA STIG's setting for the system account UID reservations.	Reserved UIDs are typically used by system software packages. If non-system accounts have UIDs in this range, they may conflict with system software, possibly leading to the user having permissions to modify system files.

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
61.	DISA	GEN000360	Group identifier reservations	Group Identifiers (GIDs) reserved for system accounts must not be assigned to non-system groups.	NRC adheres to the DISA STIG's setting for group identifier reservations.	Reserved GIDs are typically used by system software packages. If non-system groups have GIDs in this range, they may conflict with system software, possibly leading to the group having permissions to modify system files.
62.	DISA	GEN000380	GID defined in both /etc/passwd file and /etc/group file.	All GIDs referenced in the /etc/passwd file must be defined in the /etc/group file.	NRC adheres to the DISA STIG's setting for GID defined in both /etc/passwd file and /etc/group file.	If a user is assigned the GID of a group that does not exist on the system, and a group with that GID is subsequently created, the user may have unintended rights to the group.
63.	DISA	GEN008420	Memory address randomization techniques	The system must use available memory address randomization techniques.	NRC adheres to the DISA STIG's setting for memory address randomization techniques.	Successful exploitation of buffer overflow vulnerabilities relies in some measure on a predictable address structure. Address randomization techniques reduce the probability of a successful exploit.
2.14 Non AIX Security Expert Managed Recommendations – Encrypted Filesystems (EFS)						
64.	CIS	CIS-AIX 5.3-6.1: 2.14	Encrypted File (EFS) (AIX 6.1 only)	Set up EFS which are an enhancement of AIX 6.1. This enables users to encrypt their own data within a jfs2 file system.	Encryption shall be implemented according to CSO-STD-2009, "Cryptographic Control Standard."	CSO-STD-2009, "Cryptographic Control Standard" provides the NRC requirements for cryptography.
2.16 Non AIX Security Expert Managed Recommendations – General Permissions Management						

Step	Source	CIS/DISA ID	Setting Name	CIS/DISA Setting	NRC-Specific Requirement	Rationale
65.	DISA	GEN001940	User executed world-writable programs	User start-up files must not execute world-writable programs.	NRC adheres to the DISA STIG's setting for user executed world-writable programs.	If start-up files execute world-writable programs, especially in unprotected directories, they could be maliciously modified to become Trojans destroying user files or otherwise compromising the system at the user, or higher, level. If the system is compromised at the user level, compromise of the system at the root and network level eventually becomes much easier.

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.
Martian Packets	Martian packets are packets containing addresses known by the system to be invalid. Logging these messages allows the system administrator to identify misconfigurations or attacks in progress.

This page intentionally left blank.

5 ACRONYMS

AC	Access Control
ACL	Access Control List
AIX	Advanced Interactive eXecutive
AU	Audit and Accountability
CDE	Common Desktop Environment
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
EFS	Encrypted File System
FTP	File Transfer Protocol
GID	Group Identifier
IBM	International Business Machines
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISSO	Information System Security Officer
LDAP	Lightweight Directory Access Protocol
NFS	Network File System
NIM	Network Installation Management
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NRC	Nuclear Regulatory Commission
NTP	Network Time Protocol
PMTUD	Path Maximum Transmission Unit Discovery
SGI	Safeguards Information
SMB	Server Message Block
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell

STD	Standard
STIG	Security Technical Implementation Guide
SUNSI	Sensitive Unclassified Non-Safeguards Information
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UID	User Identifier

CSO-STD-1417 Change History

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