

# **USDA VULNERABILITY CHECKLIST FOR UNIX SYSTEMS**



**August 15, 2001**

**Prepared for:**

**United States Department of Agriculture  
Office of the Chief Information Officer (OCIO)**

**Prepared by:**

**Booz·Allen & Hamilton, Inc.  
3190 Fairview Park Drive  
Falls Church, VA 22042**

# USDA Vulnerability Checklist for UNIX Systems

## TABLE OF CONTENTS

<b>1. Introduction.....</b>	<b>2</b>
1.1 PURPOSE .....	2
1.2 SCOPE .....	2
1.3 BACKGROUND.....	2
1.4 REFERENCES .....	2
<b>2. Unix Vulnerability Checklist .....</b>	<b>3</b>
2.1 GENERAL HOST CONFIGURATION .....	4
2.1.1 <i>Basic Host Installation and Configuration</i> .....	5
2.1.2 <i>Accounts and Passwords</i> .....	7
2.1.3 <i>File System Security</i> .....	11
2.1.4 <i>Auditing and Logging</i> .....	13
2.1.5 <i>Backups</i> .....	15
2.2 WORKSTATION INSTALLATION AND CONFIGURATION .....	17
2.3 SERVER INSTALLATION AND CONFIGURATION.....	20
2.4 PERSONNEL.....	27
<b>Appendix A – Computer Security Requirements .....</b>	<b>28</b>
<b>Appendix B – Basic Unix Commands .....</b>	<b>34</b>
<b>Appendix C – Abbreviations.....</b>	<b>36</b>

# USDA Vulnerability Checklist for UNIX Systems

## 1. Introduction

Protection of information assets and maintaining the availability, integrity, and confidentiality of USDA information technology systems and telecommunications resources are vital in meeting USDA's program delivery requirements. Information security has emerged as a top priority for the Department of Agriculture. As technology has enhanced the ability to share information instantaneously between computers and networks, it has also made USDA organizations more vulnerable to a wider variety of threats including unlawful and destructive penetration and disruptions.

USDA's mandate for securing its information systems arises from the Computer Security Act of 1987. This law and guidance from the Office of Management and Budget (OMB) provide the Department with the basic security requirements. In addition, on May 22, 1998, the White House released Presidential Decision Directive 63 (PDD 63), which explains key elements of the policy on critical infrastructure protection. PDD 63 calls for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructure, particularly its cyber systems. These requirements, along with his own concerns, have led the Secretary to direct the Office of the Chief Information Officer (OCIO) to develop a strategy to improve USDA's cyber security. A key aspect of this strategy is the implementation of an information systems risk management program. In particular, USDA must implement a structured approach to assess risks to USDA information assets and identify vulnerabilities.

### 1.1 Purpose

This Vulnerability Checklist is designed to assist Agency Information System Security Program Managers (ISSPMs) in satisfying their responsibility to develop and implement a comprehensive risk management program as defined in Departmental Regulation (DR) 3140-001, "USDA Information Systems Security Policy." By using this guide, Agency ISSPMs can identify areas where Department Information Security requirements are not being met and develop an action plan to ensure all security requirements are satisfied.

### 1.2 Scope

This guide is to be used by all USDA organizational elements to help assess the security posture of hosts using the Unix operating system.

### 1.3 Background

Risk Assessments are mandated by OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." A security risk assessment process is a comprehensive evaluation of the system's technical and non-technical security features. It establishes the extent that a specific design and implementation meets specific security requirements.

### 1.4 References

- Public Law 100-235, "Computer Security Act of 1987"
- Public Law 93-579, "Privacy Act of 1974"

## USDA Vulnerability Checklist for UNIX Systems

- Public Law 93-502, “Freedom of Information Act”
- Public Law 99-474, “Computer Fraud and Abuse Act”
- OMB Circular No. A-130 Appendix III, “Security of Federal Automated Information Resources,” revised February 8, 1996.
- OMB Circular No. A-123, “Management Accountability and Control,” June 29, 1995.
- USDA DR 3140-001, “USDA Information Systems Security Policy” dated may 15, 1996

### 2. Unix Vulnerability Checklist

The checklist below is generic so that it should apply to most versions of Unix and Linux. However there will be occasions when the questions below do not apply in a specific instance. Also each version and type of Unix has specific vulnerabilities that are addressed in patches and upgrades. For maximum security it is imperative that the operating system and any applications or services be upgraded to the latest or most secure version as recommend by the vendor or government guidelines. This information can often be found on the vendor’s web site.

Three answers are possible when completing the checklist:

- Yes            Requirement is met
- No             Requirement is not met
- N/A            In progress, planned, or not applicable use  
                      remarks section to clarify as necessary

A “yes” answer means the host configuration adequately addresses the vulnerability in question. A “no” answer means that the vulnerability is not directly addressed but may be mitigated by other circumstances, which may be explained in the “Remarks” section. N/A means that the question is not applicable to a particular host. Again, additional details if required can be added to the “Remarks” section. It is important to note that it is extremely unlikely that a host will have all “yes” answers and all hosts assume a certain level of risk in order to be usable. Each question is numbered in order to provide traceability to the corresponding security requirements.

Appendix B provides some basic Unix commands that may be of assistance in determining the configuration of the host. The commands may not apply in all instances to all version of Unix. If a particular command does not work please see the vendor documentation for assistance.

## **USDA Vulnerability Checklist for UNIX Systems**

### 2.1 General Host Configuration

The questions in section 2.1 apply to all Unix hosts. Section 2.2 applies only to those hosts being used as workstations and Section 2.3 applies only to those hosts operating as servers.

## USDA Vulnerability Checklist for UNIX Systems

### 2.1.1 Basic Host Installation and Configuration

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Basic Host Installation and Configuration</b>					
	File servers shall be located in areas where access is restricted.	USDA COMPTSR 59			
2.1.1.1	Are mission-critical and/or sensitive workstations/servers located within an environment that has appropriate physical access controls?				
Remarks:					
	Equipment shall be protected from environmental extremes.	Best Practice			
2.1.1.2	Are temperature and humidity controls sufficient to avoid damage to the equipment?				
Remarks:					
	Controls for local area networks shall be established that prevent anyone except authorized staff from installing/removing hardware on servers/workstations.	Best Practice			
2.1.1.3	Is the Central Processing Unit (CPU) case locked and the key appropriately protected?				
Remarks:					
	Never start up (boot-up) a computer from a diskette unless it is the original write-protected system master or a trusted copy.	USDA COMPTSR 47			
2.1.1.4	Is the "boot sequence" set to start with the hard drive?				
Remarks:					
2.1.1.5	On mission-critical/sensitive workstation/servers is booting from removable media (floppy drive, CD-ROM, Zip drive, etc.) disabled and/or are the drives removed from the system?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

	Controls for local area networks shall be established that prevent anyone except authorized staff from loading software on file servers.	USDA COMPTSR 57			
2.1.1.6	Is the Basic Input Output System (BIOS)/Nonvolatile Random Access Memory (NVRAM) secured with a password?				
Remarks:					
2.1.1.7	Are the BIOS/NVRAM settings documented and stored in a secure location?				
Remarks:					
2.1.1.8	Was the host disconnected from network during installation and until appropriate security controls were in place?				
Remarks:					
2.1.1.9	Was the software used for install a legitimate copy from the manufacturer?				
Remarks:					
2.1.1.10	Are all unused ports (e.g., serial, parallel, etc.) disabled physically or in the BIOS?				
Remarks:					
	PC hard disk drives, network file servers and other media that will be used to handle agency information should be formatted between the time they are received and put into use.	USDA COMPTSR 46			
2.1.1.11	Was the system a "clean install" (i.e., started with a fresh formatted/partitioned hard drive) conducted by agency or appropriate contractor personnel?				
Remarks:					
2.1.1.12	Is the hard drive partitioning appropriate according documentation from vendor?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.1.2 Accounts and Passwords

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Accounts and Passwords</b>					
	The system will assure that users without authorization are not allowed access to the data.	USDA COMPTSR 9			
2.1.2.1	Are all default account passwords disabled or changed (e.g. root, uucp, system, etc.)?				
Remarks:					
2.1.2.2	Are all accounts that run as a single command (e.g., date, uptime, sync, and finger), disabled?				
Remarks:					
2.1.2.3	Are all open accounts such as guest removed or disabled?				
Remarks:					
2.1.2.4	Is the system configured to require root password in order to enter single user mode?				
Remarks:					
2.1.2.5	Is the system configured to restrict root login to local console?				
Remarks:					
	As soon as the system has been installed, all vendor supplied passwords, including those for software packages and maintenance accounts should be changed.	USDA COMPTSR 24			
2.1.2.6	Are all accounts with null passwords removed (i.e., accounts with no passwords)?				
Remarks:					
	Users are required to change their initial or reset passwords immediately upon login.	Best Practice			

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.1.2.7	When a new user is added and given an initial password, is the user prompted for a new password upon their initial login?				
Remarks:					
	The system shall require users to identify themselves and provide some proof that they are who they say they are (e.g., user ID and password).	USDA COMPTSR 11			
2.1.2.8	Are all users and processes whether local or remote, required to identify and authenticate themselves before being granted any access to the host?				
Remarks:					
	A password should not be shared by multiple users.	USDA COMPTSR 12			
2.1.2.9	Are all group accounts on the system (i.e., an account used by more than one user/process) except for root disabled or removed?				
Remarks:					
2.1.2.10	Are all user accounts that have the same User Identifiers (UIDs) removed or disabled?				
Remarks:					
	System users shall be provided the capability to specify, at their discretion, who (by individual users or user, groups, etc.) may have access to their data.	USDA COMPTSR 10			
2.1.2.11	Does the system provide users with discretionary access control to their data?				
Remarks:					
	The system should store passwords in a one-way encrypted form.	USDA COMPTSR 14			
2.1.2.12	Is the system configured to store passwords as hashes using an appropriately secure algorithm?				
Remarks:					
	The system should store passwords hashes in a “shadow password file”.	Best Practice			
2.1.2.13	Is the system configured to store password hashes in a protected shadow password file. (e.g., /etc/shadow/ and /etc/security/passwd.adjunct) and NOT the world readable /etc/passwd file?				
Remarks:					
	The system should automatically suppress or fully blot out the clear-text representation of the password on the data entry device.	USDA COMPTSR 15			
2.1.2.14	Does the system protect the confidentiality of the user’s password by not echoing the password on the display?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
Remarks:					
	The system should block any demonstration of password length (i.e., the cursor should not move upon input).	USDA COMPTSR 16			
2.1.2.15	Does the system protect the confidentiality of the user's password by not echoing the number of characters in the password on the display?				
Remarks:					
	Passwords and user IDs should be immediately removed when an authorized user no longer needs access to the system.	USDA COMPTSR 17			
2.1.2.16	Are procedures in place to disable/remove unnecessary and dormant accounts?				
Remarks:					
	The system should enforce password aging on a per-user basis. The system-supplied default for all non-privileged users should be no more than 60 days and no more than 30 days for user IDs that may acquire privileges. After the password aging threshold has been reached, the password shall no longer be valid and should require action by the Agency ISSPM to reset the password.	USDA COMPTSR 20			
2.1.2.17	Is the system configured to force privileged users to change passwords at least every 30 days and non-privileged users at least every 60 days?				
Remarks:					
	Passwords should not be reusable by the same individual for a period of time specified by the Agency ISSPM. The system-supplied default should be six months.	USDA COMPTSR 22			
2.1.2.18	Does the system restrict users reusing their passwords for at least six months (or as determined by the Agency ISSPM)?				
Remarks:					
	The system should provide a method of ensuring the complexity of user-entered passwords (e.g., eight characters minimum length).	USDA COMPTSR 23			
2.1.2.19	Does the system automatically enforce minimum password length of at least 8 characters?				
Remarks:					
2.1.2.20	Does the system automatically enforce minimum password complexity including both uppercase and lowercase letters, digits, and punctuation characters?				
Remarks:					
	Passwords should be periodically audited.	Best Practice			
2.1.2.21	Is password strength periodically audited by running a password-cracking program against the password hashes?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
Remarks:					
	Systems should automatically lock out an account after a fixed number of login failures.	Best Practice			
2.1.2.22	Does the system lock out an account after a number (determined by the Agency ISSPM) of failed login attempts?				
Remarks:					
	Limit the users who can promote themselves to superuser (su).	Best Practice			
2.1.2.23	If the system supports a wheel group is it implemented?				
Remarks:					
	The system must protect authentication data so that it may not be accessed by an unauthorized user.	USDA COMPTSR 33			
2.1.2.24	Are application files that might store passwords in the clear removed (e.g., .fetchmailrc or netrc)?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.1.3 File System Security

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Unix File System Security</b>					
	The system shall define and control access between named users and system resources (e.g., files and programs)	USDA COMPTSR 31			
2.1.3.1	Are all .exrc files on the system that have no legitimate purpose removed, or is the EXINIT variable employed to disable .exrc functionality?				
Remarks:					
2.1.3.2	Are any .forward files in the user home directories that may execute an unauthorized command or program?				
Remarks:					
2.1.3.3	Is the permission of /etc/utmp set to 644?				
Remarks:					
2.1.3.4	Are the permissions of /etc/sm and /etc/sm.bak set to 2755?				
Remarks:					
2.1.3.5	Is the permission of /etc/state set to 644?				
Remarks:					
2.1.3.6	Are the permissions of /etc/motd and /etc/mtab set to 644?				
Remarks:					
2.1.3.7	Is the permission of /etc/syslog.pid set to 644?				
Remarks:					
2.1.3.8	Is the kernel (e.g., /vmunix) owned by root, is the group set to 0 (or wheel) and permission set to 644?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
Remarks:					
2.1.3.9	Are /etc, /usr/etc, /bin, /usr/bin, /sbin, /usr/sbin, /tmp and /var/tmp owned by root?				
Remarks:					
2.1.3.10	Are there any unexpected world writable files or directories?				
Remarks:					
2.1.3.11	Do the files that have the SUID or SGID bit enabled require it?				
Remarks:					
2.1.3.12	Is the umask value for each user set to something reasonable (e.g., 027 or 077)?				
Remarks:					
2.1.3.13	Many default installs leave files or directories owned by bin (or sys). Have all non-setuid files and all non-setgid files and directories that are world readable but not world or group writeable and that are owned by bin been changed to ownership root with group id 0 (or wheel).				
Remarks:					
2.1.3.14	Is the system regularly checked with a security configuration auditor (e.g., COPS, Tiger, Bastille, etc.)?				
Remarks:					
2.1.3.15	Does the system have tripwire or similar program installed?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.1.4 Auditing and Logging

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Unix Auditing and Logging</b>					
	The system shall be able to record the following types of events: log on, log off, change of password, creation, deletion, opening, and closing of files, program initiation, and all actions by system operators, administrators, and security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and the success or failure of the event.	USDA COMPTSR 36			
2.1.4.1	Does the system support C2 level auditing and if so, is it implemented?				
Remarks:					
2.1.4.2	Does the system log successful logins and logouts?				
Remarks:					
2.1.4.3	Does the system log password changes?				
Remarks:					
2.1.4.4	Does the system log file system accesses including the creation, deletion, opening and closing?				
Remarks:					
2.1.4.5	Does the system log application executions?				
Remarks:					
2.1.4.6	Does the system log all actions take by system operators, administratos and security officers?				
Remarks:					
2.1.4.7	Does the system log command usage?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
Remarks:					
2.1.4.8	Does the system log successful and unsuccessful su attempts?				
Remarks:					
	For log on, log off, and password change the origin of the request (e.g., terminal ID) shall be included in the audit record. For file related events, the audit record shall include the file's name.	USDA COMPTSR 37			
2.1.4.9	For logins, logouts, and password changes, does the system record the terminal where the request originated and for file access the name of the file? These logs are usually found in the /var/adm/ or /var/log directories.				
Remarks:					
	The audit data shall be protected by the system so that read access to it is limited to those who are authorized for audit data.	USDA COMPTSR 35			
2.1.4.10	Are files sent to a central log host?				
Remarks:					
2.1.4.11	Is read/write access to the log directories (generally /var/adm or /var/log) limited to system administrators and security officers?				
Remarks:					
	The Departmental and Agency ISSPMs shall be able to selectively audit the actions of one or more users based on individual identity.	USDA COMPTSR 38			
2.1.4.12	Does the system administrator have automated tools (e.g., Swatch) to assist her/him in monitoring the logs?				
Remarks:					
	The log filters should allow extraordinary events to be reported.	Best Practice			
2.1.4.13	If logs are processed in an automated fashion are filters configured to exclude those events that are not wanted as opposed to passing only what is wanted? (This ensures that all exceptional events in the logs are reported).				
Remarks:					
	Data files should be backed up frequently and stored off-site or in a secured environment.	USDA COMPTSR 41			
2.1.4.14	Are audit logs backed up on a regular basis (to prevent both destruction and corruption)?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.1.5 Backups

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Unix Backups</b>					
	New software should be backed up immediately, retaining the original distribution diskettes in a safe and secure location. Write-protect original diskettes prior to making backup copies.	USDA COMPTSR 40			
2.1.5.1	When the system was installed were backups made of all software distributions?				
Remarks:					
	Data files should be backed up frequently and stored off-site or in a secured environment.	USDA COMPTSR 41			
2.1.5.2	Are full-backups made of the entire system on a periodic basis?				
Remarks:					
2.1.5.3	Are full-backups made of the entire system whenever this system is updated or the configuration changes?				
Remarks:					
2.1.5.4	Are the system backups adequately protected?				
Remarks:					
2.1.5.5	Are incremental backups made on a periodic basis?				
Remarks:					
2.1.5.6	For extremely critical data, are backups stored in a remote location?				
Remarks:					
	Backup media should be rotated to guard against media failure?	Best Practice			

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.1.5.7	Are the backup media rotated to guard against media failure?				
Remarks:					
	Backup media should be retired in a reasonable amount of time (see vendor recommendations) to guard against media failure.	Best Practice			
2.1.5.8	Are the backup media retired periodically to prevent eventual media failure?				
Remarks:					
	Backups should be tested periodically by restoring a few files to confirm their integrity.	Best Practice			
2.1.5.9	Are the backups tested periodically?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.2 Workstation Installation and Configuration

**Note: If the system is used as a server skip section 2.2.**

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Workstation Installation and Configuration</b>					
	The system shall define and control access between named users and system resources (e.g., files and programs)	USDA COMPTSR 31			
2.2.1	Is the host protected by a firewall?				
Remarks:					
2.2.2	Has the /etc/inetd.conf configuration file been modified to disable all unnecessary daemons?				
Remarks:					
2.2.3	Is the owner of /etc/services and etc/inetd.conf, root?				
Remarks:					
2.2.4	Are the permissions of the /etc/services file set to 644?				
Remarks:					
2.2.5	Are the permissions of the /etc/inetd.conf file set to 600?				
Remarks:					
2.2.6	Are TCP wrappers installed and set up to wrap any service that is enabled in the /etc/inetd.conf file?				
Remarks:					
2.2.7	Has the system been set up to deny all hosts by default by putting "all:all" in the /etc/hosts.deny file?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.2.8	Has a specific list of trusted hosts been put in the /etc/hosts.allow file?				
Remarks:					
2.2.9	Have allowed hosts been limited to only the services they require?				
Remarks:					
2.2.10	Have Transport Control Protocol (TCP) "banners" been set up to be displayed when a TCP port receives a connection?				
Remarks:					
2.2.11	Have TCP wrappers been enabled in PARANOID mode?				
Remarks:					
2.2.12	Are ALL "r" commands disabled (secure shell should be used in place of "r" commands)?				
Remarks:					
2.2.13	Is the Telnet server disabled or removed?				
Remarks:					
2.2.14	If secure shell (ssh) is being used, is it configured to authenticate ONLY using public/private key pair? <b>(Skip to question 2.2.17 if SSH is not installed)</b>				
2.2.15	If ssh is being used, is it configured to authenticate ONLY using public/private key pair?				
2.2.16	If ssh is installed, is it the latest patched version?				
Remarks:					
2.2.17	Has the most secure versions of all software been installed on the host?				
Remarks:					
2.2.18	Have all bug fixes and patches been downloaded and installed?				
Remarks:					
2.2.19	Has the Domain Name Service (DNS) been disabled or removed?				
Remarks:					
2.2.20	Has the sendmail daemon been disabled or removed?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
Remarks:					
2.2.21	Has the Network File System (NFS) daemon been disabled or removed?				
Remarks:					
2.2.22	Have all Hypertext Transfer Protocol (HTTP) server applications been disabled or removed?				
Remarks:					
2.2.23	Have all File Transfer Protocol (FTP) server applications been disabled or removed?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.3 Server Installation and Configuration

**Note: If the system is used as a workstation skip section 2.3.**

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Basic Server Installation and Configuration</b>					
	Controls for local area networks shall be established that prevent anyone except authorized staff from loading software on file servers.	USDA COMPTSR 57			
	The system will assure that users without authorization are not allowed access to the data.	USDA COMPTSR 9			
2.3.1	Is the host protected by a firewall?				
Remarks:					
2.3.2	Are all modems disabled or removed? <b>(Skip to question 2.3.4 if a modem is NOT installed)</b>				
2.3.3	If a modem is installed is it or the line configured not to accept incoming calls?				
Remarks:					
2.3.4	Are all unnecessary network interface cards (NICs) removed or disabled on the host?				
Remarks:					
2.3.5	Is Internet Protocol (IP) forwarding disabled (for multi-homed hosts)?				
Remarks:					
2.3.6	Is IP source routing disabled?				
Remarks:					
2.3.7	Are all remote administration type utilities removed (e.g., VNC and PCAnywhere)?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.3.8	Has the /etc/inetd.conf configuration file been modified to disable all unnecessary daemons?				
Remarks:					
2.3.9	Is the owner of /etc/services and etc/inetd.conf, root?				
Remarks:					
2.3.10	Are the permissions of the /etc/services file set to 644?				
Remarks:					
2.3.11	Are the permissions of the /etc/inetd.conf file set to 600?				
Remarks:					
2.3.12	Are TCP wrappers installed and set up to wrap any service that is enabled in the /etc/inetd.conf file?				
Remarks:					
2.3.13	Has the system been set up to deny all hosts by default by putting "all:all" in the /etc/hosts.deny file?				
Remarks:					
2.3.14	Has a specific list of trusted hosts been put in the /etc/hosts.allow file?				
Remarks:					
2.3.15	Have allowed hosts been limited to only the services they require?				
Remarks:					
2.3.16	Have TCP "banners" been set up to be displayed when a TCP port receives a connection?				
Remarks:					
2.3.17	Have TCP wrappers been enabled and configured to an appropriate security setting?				
Remarks:					
2.3.18	Has the latest version of all software been installed on the host?				
Remarks:					
2.3.19	Have all bug fixes and patches been downloaded and installed?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
Remarks:					
2.3.20	Are TCP wrappers configured to restrict access to only those hosts/subnets requiring access?				
Remarks:					
2.3.21	Are all “r” programs disabled or removed (e.g., rlogin, rsh, and rcp)? (Comment them out of /etc/inetd.conf or remove these programs completely).				
Remarks:					
2.3.22	Is telnet server disabled or removed?				
Remarks:					
2.3.23	Is the Network Time Protocol (NTP) service disabled or is access limited only to hosts within the security perimeter?				
Remarks:					
2.3.24	Is secure shell (ssh) disabled or removed? <b>(Skip to question 23.27 if SSH is NOT installed)</b>				
2.3.25	If ssh is being used, is it configured to authenticate ONLY using public/private key pair?				
2.3.26	If ssh is installed, is it the latest patched version?				
Remarks:					
2.3.27	Is the Domain Name System (DNS) service disabled or removed? <b>(Skip to question 2.3.34 if BIND is NOT installed)</b>				
2.3.28	Is it updated to the latest release?				
2.3.29	Is the primary master name server configured to perform zone transfers only to its slave servers?				
2.3.30	Are the secondary/slave servers configured not to transfer zone information to any other name servers?				
2.3.31	Are the hosts that are allowed to query a name server limited with the allow-query option?				
2.3.32	Are the interfaces that queries will be allowed on limited with the listen-on option?				
2.3.33	Is DNS set up to operate in a “chroot jail”?				
Remarks:					
2.3.34	Is the mail server disabled or removed? <b>(Skip to question 2.3.43 if a mail server is NOT installed)</b>				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.3.35	Is a more secure mail program than sendmail being used?				
2.3.36	Is the server updated to the latest version?				
2.3.37	Are the Simple Mail Transfer Protocol (SMTP) vrfy and expn commands in /etc/sendmail.cf disabled?				
2.3.38	Is relay mail disallowed in /etc/mail/access or /etc/mail/relay-domains?				
2.3.39	Are the latest versions of Post Office Protocol (POP) or Internet Mail Access Protocol (IMAP) installed?				
2.3.40	Is access to POP and IMAP controlled through TCP wrappers to limit access to only those hosts with legitimate need for the service?				
2.3.41	Are POP and/or IMAP configured to send encrypted passwords (as opposed to clear text) to authenticate? Examples would be Secure POP or Secure Sockets Layer (SSL).				
2.3.42	Is the mail server set up to operate in a "chroot jail"?				
Remarks:					
2.3.43	If printing services are not required are they removed? <b>(Skip to question 2.3.46 if printing services are NOT installed)</b>				
2.3.44	Is lpr updated to the latest version?				
2.3.45	Are the allowed remote hosts listed in /etc/hosts.lpd? PLEASE NOTE: The names of hosts allowed to use print services should be listed in /etc/hosts.lpd and not in /etc/hosts.equiv.				
Remarks:					
2.3.46	Is Network File System (NFS) disabled or removed removed? <b>(Skip to question 2.3.55 if NFS is NOT installed)</b>				
2.3.47	Is NFS updated to the latest version?				
2.3.48	Is /etc/hosts.allow configured to export directories to specific hosts?				
2.3.49	Is /etc/hosts.allow configured to export the directory "read-only" with the "ro" option?				
2.3.50	If directories are required to be exported with write access, is write access limited to hosts within administrative control?				
2.3.51	Is the /etc/exports (or the equivalent) file owned by root and does it have permissions of 644, or more restrictive?				
2.3.52	Are exported system files and directories owned by root?				
2.3.53	Are NFS clients only mounting file systems with the nosuid and nosgid options set?				
2.3.54	Are Novell servers completely restricted from mounting NFS exports?				
Remarks:					
2.3.55	Is the Server Message Block (SMB) Samba server disabled or removed? <b>(Skip to question 2.3.64 if Samba is NOT installed)</b>				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.3.56	Is the installed version the latest with all patches and updates?				
2.3.57	Is access limited to specific hosts?				
2.3.58	Are all "guest" or anonymous shares removed?				
2.3.59	Is write access to shares allowed only when absolutely necessary?				
2.3.60	Are check masks configured to ensure that default file creation is NOT world-readable? (Generally, the create mask should be 0770 and directory mask should be 0750).				
2.3.61	If Samba is required, is it configured to use encrypted passwords?				
2.3.62	If Samba is required, are entries for system accounts like bin, daemon, and ftp removed?				
2.3.63	If Samba is required, are all accounts configured with a password?				
Remarks:					
2.3.64	Is the File Transfer Protocol (FTP) service disabled or removed? ( <b>Skip to question 2.3.78 if FTP is NOT installed</b> )				
2.3.65	Is the FTP daemon updated to the most current version with all patches?				
2.3.66	Is the FTP service protected with TCP wrappers through inetd?				
2.3.67	Is anonymous access disabled?				
2.3.68	If anonymous access is needed is access configured so anonymous users cannot upload files?				
2.3.69	Is FTP access configured to allow read access only?				
2.3.70	Is the SITE EXEC command disabled?				
2.3.71	Have all command interpreters such as a shell or tools such as perl in any of the ftp directories that can be executed by SITE EXEC been removed?				
2.3.72	Has an invalid password and user shell for the ftp entry been used in the system password file and the shadow password file, (e.g. ftp:*:400:400:Anonymous FTP:/home/ftp:/bin/false)?				
2.3.73	Is logging turned on and are those files periodically reviewed?				
2.3.74	Is the FTP server configured such that ~ftp/etc/passwd does NOT contain a copy of the "real" /etc/passwd?				
2.3.75	Is the FTP server configured such that ~ftp/etc/group does NOT contain a copy of the "real" /etc/group?				
2.3.76	Is FTP configured NOT to allow the user accounts root, bin, uucp, ingress, daemon, news, nobody, and ALL vendor-supplied accounts to connect to the ftpd?				
2.3.77	Is the FTP server set up to operate in a "chroot jail"?				
Remarks:					
2.3.78	Is the web server disabled or removed? ( <b>Skip to question 2.3.91 if FTP is NOT installed</b> )				
2.3.79	Has the web server been configured so that basic access to all directories and files on the server is DENIED by default?				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.3.80	Have all sample code, pages and scripts been removed?				
2.3.81	Has remote administration been disabled?				
2.3.82	Is the web server configured to run as a user with extremely limited rights and accesses (e.g., NOT running as root)?				
2.3.83	Have allow Computer Gateway Interface (CGI) execute permissions been implemented only on the CGI directories?				
2.3.84	Has write access on HTML directories been removed?				
2.3.85	Are automatic directory listings disabled?				
2.3.86	Is it configured NOT to follow symbolic links?				
2.3.87	Is it configured to prohibit server-side includes?				
2.3.88	Is it configured to use SSL for sensitive data and authentication?				
2.3.89	Is logging enabled and are those logs periodically reviewed?				
2.3.90	Is the web server set up to operate in a "chroot jail"?				
Remarks:					
2.3.91	Is the Network Information Service (NIS) disabled or removed? <b>(Skip to question 2.3.98 if NIS is not installed)</b>				
2.3.92	Are the NIS maps protected through hard-to-guess domain names?				
2.3.93	Is Yppassword disabled?				
2.3.94	Is Ypbind configured to run on a reserved or privileged port?				
2.3.95	Is Nisd or yp.nisd configured to run on a reserved or privileged port?				
2.3.96	Is Ypserv, configured to run on a reserved or privileged port?				
2.3.97	Are the latest versions of YP installed?				
Remarks:					
2.3.98	Is X Windows is not required is it disabled or removed? <b>(Skip to question 2.3.103 if X Windows is NOT installed)</b>				
2.3.99	Is each X Windows host configured to write a .Xauthority file, or the equivalent, into each X Windows user's home directory?				
2.3.100	Are X Clients that are authorized to connect to X Server display listed in the X*.hosts, or equivalent file(s) if the .Xauthority utility is not used?				
2.3.101	Is the xhost + command disabled?				
2.3.102	Is the sticky bit set on all .X11* directories under /tmp?				
Remarks:					
2.3.103	Is Simple Network Management Protocol (SNMP) disabled or removed? <b>(Skip to question 2.3.107 if SNMP is NOT installed)</b>				

## USDA Vulnerability Checklist for UNIX Systems

Number	Requirement	Source	Y	N	N/A
2.3.104	Are SNMP passwords changed from the default and are they sufficiently hard to guess?				
2.3.105	Are the permissions of snmpd.conf files set to 700, or more restrictive?				
2.3.106	Are the Management Information Base (MIB) file permissions set to 700, or more restrictive?				
Remarks:					
2.3.107	Is the server periodically scanned with a vulnerability assessment tool (e.g. Nessus, Saint, ISS, etc.)?				
Remarks:					
	All software (operating system and applications) should be kept up-to-date as security patches become available.	Best Practice			
2.3.108	Is all software installed updated to the latest level as recommend by the vendor?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### 2.4 Personnel

Date: \_\_\_\_\_ / \_\_\_\_\_ / \_\_\_\_\_

Hostname: \_\_\_\_\_

IP Address: \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_ . \_\_\_\_\_

Operating System: \_\_\_\_\_

OS Version: \_\_\_\_\_

Number	Requirement	Source	Y	N	N/A
<b>Basic Server Installation and Configuration</b>					
	All personnel should be appropriately qualified both in systems administration and security.	Best Practice			
2.4.1	Are all end users notified of their responsibilities (e.g., protect their passwords, report suspicious activity, etc.)?				
Remarks:					
2.4.2	Do all system administrators have appropriate experience and/or certifications to support the security requirements of the host?				
Remarks:					
2.4.3	Is the training budget adequate for maintaining the skills of systems administrators?				
Remarks:					

## USDA Vulnerability Checklist for UNIX Systems

### Appendix A – Computer Security Requirements

#### Computer Security Requirements

Requirement No	Requirement	Allocation
1	Personally-owned computers or software will not be used to process, access, or store sensitive information without the approval of the Agency ISSPM.	AIS
2	Configuration control plans shall be prepared and configuration management shall be implemented in all critical, sensitive and foreign intelligence AIS and networks.	AIS
3	Configuration control should begin in the earliest stages of the design and development of the system or network and extend over the full life of the configuration items included in the design and development stages.	AIS
4	For every change that is made to an AIS or network, the design and requirements of the changed version of the system should be identified.	AIS
5	Every change made to documentation, hardware, and software/firmware should be reviewed and approved by the Agency ISSPM, Network Security Officer, or the available security staff.	Bureau or Agency
6	Configuration status accounting is responsible for recording and reporting on the configuration of the project throughout the change.	AIS
7	Through the process of a configuration audit, the completed change can be verified to be functionally correct, and for trusted systems and networks, consistent with the security policy of the system or network.	AIS
8	In the case of a change to hardware or software/firmware that will be used at multiple sites, configuration control is also responsible for ensuring that each site receives the appropriate version of the system or network.	Bureau or Agency
9	The system will assure that users without authorization are not allowed access to the data.	AIS
10	System users shall be provided the capability to specify, at their discretion, who (by individual users or user, groups, etc.) may have access to their data.	AIS
11	The system shall require users to identify themselves and provide some proof that they are who they say they are (e.g., user ID and password).	AIS

## USDA Vulnerability Checklist for UNIX Systems

### Computer Security Requirements

Requirement No	Requirement	Allocation
12	A password should not be shared by multiple users.	AIS
13	The system should prevent a user from choosing a password that is already associated with another user ID.	AIS
14	The system should store passwords in a one-way encrypted form.	AIS
15	The system should automatically suppress or fully blot out the clear-text representation of the password on the data entry device.	AIS
16	The system should block any demonstration of password length (i.e., the cursor should not move upon input).	AIS
17	The system, by default, should not allow null passwords during normal operation.	AIS
18	Passwords and user IDs should be immediately removed when an authorized user no longer needs access to the system.	Bureau or Agency
19	The system should provide a mechanism to allow passwords to be user-changeable.	AIS
20	The system should enforce password aging on a per-user basis. The system-supplied default for all non-privileged users should be no more than 60 days and no more than 30 days for user IDs that may acquire privileges. After the password-aging threshold has been reached, the password shall no longer be valid and should require action by the Agency ISSPM to reset the password.	Bureau or Agency
21	The system should provide a mechanism that notifies the user to change their password.	AIS
22	Passwords should not be reusable by the same individual for a period of time specified by the Agency ISSPM. The system-supplied default should be six months.	AIS
23	The system should provide a method of ensuring the complexity of user-entered passwords (e.g., eight characters minimum length).	AIS
24	As soon as the system has been installed, all vendor supplied passwords, including those for software packages and maintenance accounts should be changed.	AIS
25	Terminals, workstations and networked personal computers should never be left unattended when user ID and password have been logged in.	Bureau or Agency

## USDA Vulnerability Checklist for UNIX Systems

### Computer Security Requirements

Requirement No	Requirement	Allocation
26	AISs and networks which process, store, or transmit sensitive information shall meet the requirements for C2 level protection as evaluated by the National Security Agency or the National Institute for Standards and Technology.	AIS
27	If a network is accessed by a user who is not authorized to use all or some of the sensitive information processed by or communicated over the network (or if the network is accessed by dial-up circuits), C2 protection shall be implemented on microprocessors running UNIX or other multi-user, multi-tasking operating systems.	AIS
28	Until C2 products are available, interim discretionary access control protection measures for microcomputers shall be implemented.	AIS
29	As an interim measure, specialized automated techniques shall be used to verify the proper output classification of data until the incorporation of trusted products is feasible, or a new AIS can be designed and implemented to meet the specified level of trust.	AIS
30	When a storage object (e.g., core area, disk file, etc.) is initially assigned, allocated, or reallocated to a system user, the system shall assure that it has been cleared.	AIS
31	The system shall define and control access between named users and system resources (e.g., files and programs)	AIS
32	Sensitive AIS and networks shall be protected to at least the minimum level of controlled access protection (C2) .	AIS
33	The system must protect authentication data so that it may not be accessed by an unauthorized user.	AIS
34	The system shall be able to create, maintain, and protect from modification, unauthorized access, or destruction an audit trail of accesses to the resources it protects.	AIS
35	The audit data shall be protected by the system so that read access to it is limited to those who are authorized for audit data.	AIS

## USDA Vulnerability Checklist for UNIX Systems

### Computer Security Requirements

Requirement No	Requirement	Allocation
36	The system shall be able to record the following types of events: log on, log off, change of password, creation, deletion, opening, and closing of files, program initiation, and all actions by system operators, administrators, and security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and the success or failure of the event.	AIS
37	For log on, log off, and password change the origin of the request (e.g., terminal ID) shall be included in the audit record. For file related events, the audit record shall include the file's name.	AIS
38	The Departmental and Agency ISSPMs shall be able to selectively audit the actions of one or more users based on individual identity.	Bureau or Agency
39	Audit procedures shall be developed and coordinated with other internal control procedures required under OMB Circular A-123.	Bureau or Agency
40	New software should be backed up immediately, retaining the original distribution diskettes in a safe and secure location. Write-protect original diskettes prior to making backup copies.	AIS
41	Data files should be backed up frequently and stored off-site or in a secured environment.	Bureau or Agency
42	Damaged software programs should be restored from the original diskettes, not from regular backups.	AIS
43	Use only new media for making copies for distribution.	AIS
44	PC machine-readable media should be scanned for malicious software before initial use. Write-protect software prior to scanning to prevent possible contamination from system and virus scan software being used.	Facility
45	Software obtained electronically from bulletin boards shall be downloaded to newly formatted diskettes and not directly to the computer hard disk.	Facility
46	PC hard disk drives, network file servers and other media which will be used to handle agency information should be formatted between the time they are received and put into use.	Facility

## USDA Vulnerability Checklist for UNIX Systems

### Computer Security Requirements

Requirement No	Requirement	Allocation
47	Never start up (boot-up) a computer from a diskette unless it is the original write-protected system master or a trusted copy.	Facility
48	Portable computer systems, such as laptops, that leave agency controlled areas shall be scanned for viruses before and after connecting to systems or software owned by other organizations.	Facility
49	The decision to safeguard sensitive storage media during its life cycle should be based on a risk analysis to access the threat to the sensitive information.	Bureau or Agency
50	A purge is not complete until a final overwrite is made using unclassified data.	AIS
51	Media should be purged before submitting it for destruction.	AIS
52	Degaussing with an approved degausser is the only method acceptable for purging classified or unclassified intelligence information media.	AIS
53	Overwrite software shall be protected at the level of the media it purges. The overwrite software must be protected from unauthorized modification.	AIS
54	Magnetic tape should have a label applied to the reel that identifies the coercivity of the media. Labels that show the classification should not be removed from the reel until the media is declassified.	Facility
55	Leased equipment containing non-removable magnetic storage media should not be returned to the vendor unless the media is declassified using an approved procedure.	Facility
56	Once sensitive information has been written to the hard-drive of a personally owned computer, the sensitive data shall be completely erased when it is no longer needed on the system to preclude disclosure or data corruption.	Bureau or Agency
57	Controls for local area networks shall be established that prevent anyone except authorized staff from loading software on file servers.	Facility
58	A local area network file server shall never be used as a workstation.	Facility
59	File servers shall be located in areas where access is restricted.	Facility

## USDA Vulnerability Checklist for UNIX Systems

### Computer Security Requirements

Requirement No	Requirement	Allocation
60	Security Features User's Guide: A single summary, chapter, or manual in user documentation shall describe the security features provided by the Trusted Computing Base, guidelines on their use and how they interact with one another.	AIS
61	A Trusted Facility Manual: A manual addressed to the ADP security administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.	Facility
62	Test documentation: The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.	AIS
63	Design documentation: Documentation shall be available that provides a description of the manufacturers philosophy of protection and an explanation of how this philosophy is translated into the Trusted Computing Base (TCB). If the TCB is composed of distinct modules, the interfaces between these modules shall be described.	AIS
64	The stand-alone hardware should be scanned before it is used by the vendor to verify that the computer does not contain any viruses.	Bureau or Agency
65	The stand-alone hardware should be scanned when the demonstration is completed to determine if the vendor software contains a virus and remove it from the system.	Bureau or Agency
66	Written certification from the vendor that the demonstration software has been checked and is free from viruses shall be obtained prior to loading any vendor software.	Bureau or Agency

# USDA Vulnerability Checklist for UNIX Systems

## Appendix B – Basic Unix Commands

**apropos** <subject> – Provides a listing of all the man pages that have to do with the *subject*

**bg** <number> – Starts job *number* in background again

**cd** <hello> – Changes to directory *hello* inside current directory

**cd** / – Changes directory to /

**cd** ~ – Changes directory to user's home directory

**cd** ../<dirname> – Change to directory *dirname* one directory above current directory

**cd** ../../<dirname> – Changes to directory *dirname* two directories above current directory

**cd** - – Changes directory to the last directory

**cd** .. – Moves one directory up

**clear** – Clears the terminal screen

**cp** <source> <destination> – Copies files from *source* to *destination*, options like *-rf* also work

**Ctrl-c** – Terminates current process or application

**Ctrl-z** – Terminates a job

**df** – Shows memory usage for every partition and mounted file system

**dir** – Lists directory contents similar to “ls” but with fewer options.

**du** – Shows disk usage

**du -b --total** – Shows the size of a directory and its contents

**fg** <number> – Starts job *number* in foreground

**find** <directory> -name <name> – Finds a file with *name* in the filename starting at *directory*

**grep -i** <text string> </directory/to/start> – Searches (non case sensitive) for *text string* in a file starting at *directory/to/start*

**head** *filename* – Lists the first 10 lines of a filename

**head -x** *filename* – Lists the first x lines of a filename

**jobs** – Lists all the jobs (along with numbers) you currently have running

**kill** <pid> – Kills a process based on process ID

**less** – Allows scrolling through a file a page at a time

**ln -s** </home/joeuser> <myalias> – Creates an alias to */home/joeuser*

**ls -a** – Lists all files, including those that start with a period, ‘.’

**ls -l** – Provides a detailed listing of directory, including file attributes and permissions

**ls | sort -r | less** – Sorts the directory in reverse alphabetical order and provides output a screen at a time

**ls** > <filename> – Redirects the output of a command into file *filename*

**ls** >> <filename> – Redirects the output of a command and appends to file *filename*

**ls -l | tee** <filename> – Sends the output of the ls to the screen and to *filename*

**man** <command> – Displays manual page for *command*

**mkdir** <name1> <name2> ... <namex> – Makes directories with names *name1, name2, ..., namex* where specified or default current directory

**more** – Allows scrolling through a file a page at a time

**mv** <file1> <file2> – Moves file from one location to another, can also be used to rename a file

**passwd** – Changes password

**passwd** <username> – Changes password for specified *username*

**ps** – Displays all processes users have started

**ps au** – Displays all processes for all users

**pwd** – Displays the current directory

**rcp** – Copies files from another host

**reboot** – Reboots local host

**rm** <filename> – Deletes a file

**rm -rf** <directory-name> – Forces recursive removal of directory with no prompting

**rmdir** – Deletes a directory

**TAB** – Completes filenames or directories when typing a command

**tail** *filename* – Displays the last 10 lines of a filename

**tail -x** *filename* – Displays the last x lines of a filename

## USDA Vulnerability Checklist for UNIX Systems

**tee** – Sends output to screen and a file when used with pipe

**top** – Lists all operations in progress and gives options to sort based on usage along with other options

**tree** – Displays graphical representation of directory structure

**w** – Displays who is logged on

**!*string***> – Executes the most recent command that began with *string*

**!?*string***> – Executes the last command with *string* anywhere in the command

| Pipes the output of the first command to the input of another (e.g., ls | more)

> Sends the output of a command to a specified file (e.g., ls > myfile)

>> Appends the output of a command to a specified file (e.g., ls >> myfile)

& Runs the command in the background (e.g., netscape &)

~ Designates the home directory (e.g., echo ~)

< Designates input from somewhere other than terminal program (e.g., < input)

\* Designates any string of characters (e.g., ls \*.c)

? Designates any single character (e.g., ls file?)

To identify world writable files or directories, use the commands:

```
# /bin/find / -type f \ ( -perm -2 -o -perm -20 \) -exec ls -lg {} \
```

```
# /bin/find / -type d \ ( -perm -2 -o -perm -20 \) -exec ls -lg {} \
```

To identify files that have the SUID or SGID bit enabled, use the command:

```
# /bin/find / -type f \ ( -perm -004000 -o -perm -002000 \) \ -exec ls -lg {} \
```

## USDA Vulnerability Checklist for UNIX Systems

### Appendix C – Abbreviations

BIOS – Basic Input Output System  
CGI – Computer Gateway Interface  
COMPTSR – Computer Security Requirements  
CPU – Central Processing Unit  
DNS – Domain Name Service  
FTP – File Transfer Protocol  
HTTP – Hypertext Transfer Protocol  
IMAP – Internet Mail Access Protocol  
IP – Internet Protocol  
ISSPM – Information System Security Program Manager  
MIB – Management Information Base  
NIC – Network Interface Card  
NIS – Network Information System  
NFS – Network File System  
NTP – Network Time Protocol  
NVRAM – Nonvolatile Random Access Memory  
OMB – Office of Management and Budget  
OS – Operating System  
PDD – Presidential Decision Directive  
POP – Post Office Protocol  
SMB – Server Message Block  
SMTP – Simple Mail Transfer Protocol  
SNMP – Simple Network Management Protocol  
SSH – Secure Shell  
SSL – Secure Socket Layer  
TCP – Transport Control Protocol  
UID – User Identifiers  
USDA – United States Department of Agriculture  
VNC – Virtual Network Computing