DRAFT

UNIX

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 5, Release 0

7 October 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

LIST OF TABLES

SUMMARY OF CHANGES

Version 5, Release 0 of this *STIG* includes text modifications and revisions to all sections relative to the previous release that was Version 4, Release 4, dated 9 September 2003. To avoid confusion over the amount of modifications to the text, a table has been included to track the status of PDIs, new PDIs are detailed, and deletions and/or modification of appendixes have been noted. Text modifications are to be assumed for each section within this *STIG*. Support for SuSE, Solaris 10, and IRIX has been integrated in this release. Minimal changes have been made to *Section 15, MQ Series 5.2*.

Table to Display Status of Old PDIs

IAVA Related PDIs are mentioned in this table, but are not included in this *STIG*. These PDIs are detailed in the *UNIX Checklist*. Details are provided below to allow the user community a tracking mechanism for comparison.

Old PDI Number	New PDI Number	Removed	IAVA Related
AA002	G049		
AD16	G087		
A028	G389		
G001	G001		
G002	G003		
G003	G005		
G004	G055		
G006	G023		
G007	G025		
G008	G027		
G009	G029		
G010	G037		
G011	G039		
G012	G041		
G013	G043		
G014	G045		
G015	G047		
G016	G051		
G018	G057		
G019	G059, G061, G063, G065, G067, G069		
G020	G071, G073, G079		
G021	G089		
G022	G091		
G023	G093		
G024	G095		
G025	G097		
G026	G099		
G027	G105		

Old PDI Number	New PDI Number	Removed	IAVA Related
G029	G033		
G030	G035		
G031	G673		
G033	G115		
G034	G117		
G035	G119		
G036	G121		
G037	G129		
G038	G183		
G039	G135		
G040	G137		
G041	G139		
G042	G131		
G043	G133		
G044	G123		
G045	G125		
G046	G127		
G047	G143		
G048	G141		
G049		X	
G050	G145		
G051	G147		
G052	G149		
G053	G151		
G054	G153		
G055	G155		
G056	G199		
G057	G201		
G058	G161		
G059	G163		
G060	G205		
G061	G165		
G062	G167		
G066	G213		
G067	G157		
G068	G159		
G069	G225		
G070	G227		
G071	G077		
G072	G229		
G073	G231		
G074	G233		
G075	G235		
G076	G239		

Old PDI Number	New PDI Number	Removed	IAVA Related
G077	G241		
G078	G243		
G079	G261		
G082	G251		
G083	G257		
G084	G253		
G085	G259		
G086	G255		
G087	G263		
G088	G265		
G089	G269		
G090	G271		
G092	G277		
G093	G279		
G094	G281		
G095	G283		
G100	G287		
G101	G289		
G102	G291		
G103	G293		
G104	G295		
G105	G297		
G106	G299		
G107	G393		
G108	G395		
G109	G397		
G110	G399		
G112	G181		
G113		X	
G120	G409		
G121	G411		
G122	G413		
G123	G415		
G125	G459		
G127	G461		
G128	G463		
G131	G465		
G132	G467		
G133	G469		
G134	G471		
G135	G473		
G136	G475		
G137	G477		
G140	G513		

Old PDI Number	New PDI Number	Removed	IAVA Related
G141	G515		
G142	G517		
G143	G519		
G144	G521		
G145	G523		
G147	G507		
G149	G533		
G150	G535		
G151	G537		
G152	G541		
G155		X	
G157		X	
G158		X	
G159		X	
G160		X	
G161		X	
G162		X	
G163		X	
G164		X	
G165		X	
G166		X	
G167		X	
G168		X	
G170		X	
G172		X	
G173	G655		
G174	G651		
G176	G657		
G177	G593		
G178	G595		
G179	G597		
G180	G599		
G181	G601		
G182	G603		
G183	G605		
G184	G607		
G185	G609		
G186	G611		
G188	G675		
G189	G677		
G190	G679		
G196	G683		
G197	G685		
G198	G401		

Old PDI Number	New PDI Number	Removed	IAVA Related
G200	G315		
G201	G317		
G203	G319		
G204	G321		
G205	G327		
G206	G329		
G207	G331		
G208	G333		
G209	G335		
G210	G337		
G211	G347		
G212	G349		
G213	G351		
G214	G353		
G215	G355		
G216	G357		
G220	G613		
G221	G615		
G222	G617		
G224	G553		
G225	G555		
G226	G557		
G229	G109		
G234	G007		
G345	G800		X
G357	G801		X
G361	G802		X
G363	G803		X
G365	G804		X
G371	G805		X
G373	G806		X
G499	G111		
G500	G113		
G501	G245		
G502	G247		
G503	G313		
G504	G249		
G505	G807		X
G507	G808		X
G508	G809		X
G509	G810		X
G510	G811		X
G511	G079		
G512	G812		X

Old PDI Number	New PDI Number	Removed	IAVA Related
G513	G813		X
G514	G814		X
G515	G815		X
G516	G816		X
G517	G817		X
G518	G818		X
G519	G819		X
G520	G820		X
G521	G821		X
G522	G822		X
G523	G823		X
G524	G824		X
G525	G825		X
G527	G826		X
G529	G827		X
G531	G828		X
G533	G829		X
G535	G830		X
G537	G831		X
G541	G832		X
G543	G833		X
G545	G834		X
G547	G835		X
G549	G836		X
G551	G837		X
G553	G838		X
G555	G839		X
G559	G840		X
G561	G841		X
G563	G842		X
G567	G843		X
G569	G844		X
G573	G845		X
G575	G846		X
G577	G847		X
G578	G848		X
G579	G849		X
G580	G850		X
G581	G851		X
G582	G852		X
G583	G853		X
G584	G854		X
G585	G855		X
G586	G856		X

Old PDI Number	New PDI Number	Removed	IAVA Related
G587	G857		X
G588	G858		X
G589	G859		X
G590	G860		X
G591	G861		X
G592	G862		X
G593	G863		X
G594	G864		X
G595	G865		X
G596	G866		X
G597	G867		X
G598	G868		X
G599	G869		X
G605	G053		
G606	G081		
G609	G207		
G610	G209		
G611	G169		
G612	G171		
G613	G173		
G614	G215		
G615	G219		
G616	G221		
G617		X	
G618		X	
G620	G339		
G621	G341		
G622	G343		
G623	G345		
G625	G359		
G626	G361		
G627	G363		
G629	G365		
G630	G367		
G631	G417		
G632	G419		
G633	G421		
G634	G423		
G635	G425		
G636	G427		
G637	G429		
G638	G431		
G639	G433		
G640	G435		

Old PDI Number	New PDI Number	Removed	IAVA Related
G641	G437		
G642	G439		
G643	G441		
G644	G443		
G645	G479		
G646	G481		
G647	G483		
G648		X	
G649	G525		
G650	G527		
G653		X	
G655	G561		
G656	G563		
G657	G565		
G658	G569		
G661	G577		
G662	G579		
G663	G663		
G666		X	
G670		X	
G671		X	
G673		X	
G674	G301		
G677	SO05		
G678	SO07		
G679	SO09		
G680	SO11		
G681	SO13		
G682	SO15		
G685	SO17		
G687	SO29		
G689	G383		
G690	G385		
G691	G085		
G692	SO41		
G695	G021		
G696	SO43		
G698	G101		
G699		X	
G700	G285		
G701	G571		
L001	G870		X
L003	L001		
L007	L003		

Old PDI Number	New PDI Number	Removed	IAVA Related
L010	G871		X
L013		X	
L017	L021		
L022	L027		
L026		X	
L032	L041		
L034	L043		
L040	G649		
L042		X	
L044	L047		
L045	L049		
L046	L051		
L048	G631		
L050	G633		
L051	G635		
L052	G637		
L053		X	
L054	G639		
L055	G641		
L056	G645		
L057	G643		
L058		X	
L060		X	
L064	L005		
L066	L007		
L068	L009		
L072	L011		
L074	L013		
L076		X	
L078	L015		
L080	L019		
L082		X	
L084	L023		
L088	L025		
L106		X	
L110		X	
L126		X	
L128	L033		
L138		X	
L140	L035		
L142	L037		
L144		X	
L152		X	
L154	G651		

Old PDI Number	New PDI Number	Removed	IAVA Related
L156	G653		
L158	G655		
L160	G657		
L162	G659		
L164	G661		
L168	L053		
L170	G629		
L174	G647		
L184		X	
L188		X	
L190		X	
L192		X	
L194		X	
L196		X	
L198		X	
L200		X	
L202		X	
L204	L055		
L206	L057		
L208	L059		
L210		X	
L212		X	
L214	L063		
L216		X	
L220		X	
L222		X	
L224		X	
L230	L067		
MQ01			
MQ02			
MQ03			
MQ04			
MQ05			
MQ06			
MQ07			
MQ08			
MQ09			
MQ10			
MQ11			
MQ12			
MQ13			
MQ14			
MQ15			
MQ16			

Old PDI Number	New PDI Number	Removed	IAVA Related
MQ17			
MQ18			
MQ19			
MQ20			
MQ21			
MQ22			
MQ23			
MQ24			
MQ25			
MQ26			
MQ27			
MQ28			
MQ30			
MQ31			
MQ32			
MQ33			
NS01	G619		
NS03	G621		
SC01		X	
SC02		X	
SC03		X	
SC04		X	
SC05		X	
SC06		X	
SC07		X	
SC08		X	
SC09		X	
SC10		X	
SG01	G872		X
SG03	G873		X
SG05	G874		X
SO01		X	
SO05	SO19		
SO06	SO21		
SO07	SO23		
SO08	SO25		
SO09	SO27		
SO10	SO31		
SO25		X	
SO26		X	
SO27		X	
SO28		X	
SO29		X	
HP01		X	

Old PDI Number	New PDI Number	Removed	IAVA Related
HP02	HP03		
HP03		X	
HP04		X	
HP05		X	
HP06		X	
HP07	HP09		
HP08	HP07		
HP09	HP11		
HP10		X	
HP11		X	
HP12		X	
HP13		X	
HP14	HP05		
AIX01		X	
AIX02	AIX03		
AIX03		X	
AIX04		X	
AIX05		X	
AIX06		X	
AIX07	AIX05		
AIX08		X	
AIX09		X	
AIX10	AIX07		
T01		X	
T02		X	
T03		X	
T05		X	
T06		X	
T07		X	
V042	G403		
V046	G407		
V052	G509		
V064	G875		X
V102	G405		
V124	G485		
V125	G487		
V126	G489		
V128	G491		
V130	G493		
V131	G495		
V141	G539		
V145	G551		
V155	G545		
V2345	G876		X

Old PDI Number	New PDI Number	Removed	IAVA Related
V324	G877		X
V3375	G878		X
V5899	G583		
V9402	IRIX03		
V9478	G585		
V9482	G587		
V9517	G591		
V9730	G589		
V9756	SO37		
V9758	SO39		
W01	G445		
W03	G447		
W07	G449		
W09	G451		
W11	G453		
W13	G455		
W17	G457		
W27		X	

Table 0-1. Status of Old PDIs

New PDIs

The below mentioned new PDIs encompass PDIs that were previously designated with an N/A, PDIs that have been reworked to better ensure the security requirements are met, and new PDIs that reflect the Center of Internet Security (CIS) Benchmarks as well as new security data for some UNIX platforms.

- *(G009: CAT I) The IAO will ensure the operating system is a supported release.*
- *(G011: CAT II) The SA will create and maintain a system baseline (all device files, sgid and suid file, and system libraries and binaries), to include cryptographic hashes of files in the baseline.*
- *(G013: CAT II) The SA will maintain all baseline backups on write-protected media.*
- *(G015: CAT II) The SA will execute a new system baseline after every software change.*
- *(G017: CAT II) The SA will execute a new system baseline after changes to system directories and files are applied.*
- *(G019: CAT II) The SA will ensure the accuracy of the system clock and date.*

- *(G031: CAT II) The SA will ensure uids 0 – 99 (0 – 499 for Linux) are reserved for system accounts.*

- *(G083: CAT II) The SA will ensure the system global password configuration files are configured per password requirements.*

- *(G103: CAT II) The IAO will enforce users requiring root privileges to log on to their personal account and invoke the /bin/su - command to switch user to root.*

- *(G175: CAT II) The SA will ensure global initialization files have permissions of 644, or more restrictive.*

- *(G177: CAT II) The SA will ensure the owner of global initialization files is root.*

- *(G179: CAT II) The SA will ensure the group owner of global initialization files is root, sys, bin, other, or the system default.*

- *(G185: CAT II) The SA will ensure the owner of all default/skeleton dot files is root or bin.*

- *(G187: CAT II) The user and SA will ensure global initialization files do not have a* ***'.'****, or a* ***'::'*** *in the PATH variable definition except as the last entry.*

- *(G203: CAT II) The user and SA will ensure local initialization files do not have a* ***'.'****, or a* ***'::'*** *in the PATH variable definition except as the last entry.*

- *(G211: CAT II) The SA will ensure .rhosts, .shosts, /etc/passwd, /etc/shadow, /etc/group, and hosts.equiv files do not contain a plus (+) unless defining entries for NIS+ netgroups.*

- *(G217: CAT I) The SA will ensure neither .rhosts nor .shosts are used, unless justified and documented with the IAO.*

- *(G223: CAT II) The SA will ensure .rhosts is not supported in the pluggable authentication module (PAM).*

- *(G237: CAT III) All device files will be located in the directory trees as installed and designated by the operating system and/or application vendor.*

- *(G267: CAT II) The SA will ensure the group owner of public directories is root, sys, bin, or the application group.*

- *(G273: CAT II) The SA will ensure development systems are subject to the same security requirements as production systems.*

- *(G275: CAT I) The SA will immediately change any default passwords.*

- *(G303: CAT II) The IAO will ensure the auditing software can record the following for each audit event:*

  - *Date and time of the event*
  - *Userid that initiated the event*
  - *Type of event*
  - *Success or failure of the event*
  - *For I&A events, the origin of the request (e.g., terminal ID)*
  - *For events that introduce an object into a user's address space, and for object deletion events, the name of the object, and in MLS systems, the object's security level.*

- *(G305: CAT II) Auditing will be configured to immediately alert personnel of any unusual or inappropriate activity with potential IA implications.*

- *(G307: CAT III) The IAO will ensure audit files are retained at least one year; systems containing SAMI will be retained for five years.*

- *(G309: CAT III) The IAO will ensure audit files are backed up no less than weekly onto a different system or media than the system being audited.*

- *(G311: CAT II) On a daily basis, the IAO will review the audit trails and/or system logs for the following:*

  - *Excessive logon attempt failures by single or multiple users*
  - *Logons at unusual/non-duty hours*
  - *Failed attempts to access restricted system or data files indicating a possible pattern of deliberate browsing*
  - *Unusual or unauthorized activity by System Administrators*
  - *Command-line activity by a user that should not have that capability*
  - *System failures or errors*
  - *Unusual or suspicious patterns of activity*

- *(G323: CAT II) The SA will ensure the owner of crontabs is root or the crontab creator.*

- *(G325: CAT II) The SA will ensure default system accounts (with the possible exception of root) are not listed in the cron.allow file. If there is only a cron.deny file, the default accounts (with the possible exception of root) will be listed there.*

- *(G369: CAT III) The SA will ensure core dumps are disabled or restricted.*

- *(G371: CAT III) The SA will ensure the owner and group owner of the core dump data directory is root and permissions of 700, or more restrictive.*

- *(G373: CAT II) The SA will ensure the executable stack is disabled.*

- *(G375: CAT II) The SA will ensure NFS client requests are restricted.*

- *(G377: CAT II) The SA will ensure better TCP sequence numbers are used.*

- *(G379: CAT II) The SA will ensure network parameters are securely set.*

- *(G381: CAT III) The SA will configure separate filesystem partitions for /home, /export/home, and /var unless justified and documented with the IAO.*

- *(G387: CAT II) The SA will ensure the authentication notice and informational data is logged.*

- *(G391: CAT II) The SA will ensure inetd is disabled (xinetd for Linux) if all inetd-based services are disabled.*

- *(G497: CAT II) The SA will ensure FTP and telnet within an enclave is behind the premise router and protected by a firewall and router access control lists.*

- *(G499: CAT II) The SA will ensure FTP and telnet within an enclave is justified and documented with the IAO.*

- *(G501: CAT I) The SA will ensure FTP and telnet from outside the enclave into the enclave is not permitted, unless encrypted and the following conditions apply:*

  - *FTP and telnet are acceptable from outside the enclave through a remote access Virtual Private Network (VPN). The connection will terminate outside the firewall so as to not bypass the security architecture. The connection will be proxied at the firewall or via an FTP/telnet proxy.*

  - *FTP and telnet are acceptable via a site-to-site VPN between trusted enclaves; however, the risk will be accepted as part of the accreditation package, System Security Authorization Agreement (SSAA) or an Acceptance of Risk letter (AORL) must already be in place for the tunnel. FTP and telnet are acceptable within distributed enclaves, if required, as long as the traffic is physically or logically segregated from normal traffic*

using a method supported by the network technology to create a virtual connection (e.g., VLAN, VPN, LANE, MPLS, IPSec tunnels).

- *(G503: CAT I) The SA will ensure userids/passwords used for FTP and telnet do not have administrative or root privileges.*
- *(G505: CAT II) The IAO will ensure an AORL is used to document the use of unencrypted FTP and telnet or the risk will be accepted as part of the accreditation package.*
- *(G511: CAT II) The SA and IAO will ensure an anonymous ftp server houses only public information.*
- *(G529: CAT II) The SA will ensure the ftp users umask is 077.*
- *(G531: CAT I) The SA will ensure fsp is not enabled.*
- *(G543: CAT II) The SA will ensure .Xauthority files have permissions of 600, or more restrictive.*
- *(G547: CAT II) X Clients that are authorized to connect to X Server display will be listed in the X*.hosts, or equivalent file(s) if the .Xauthority utility is not used.*
- *(G549: CAT II) The SA will ensure remote X-terminal access host will be limited to authorized X clients.*
- *(G559: CAT II) The SA will ensure the owner of the snmpd.conf file is root with a group owner of sys and the owner of MIB files is root with a group owner of sys or the application.*
- *(G567: CAT II) The SA will ensure local hosts are not configured to act as loghosts for systems outside the local network.*
- *(G573: CAT I) The SA and IAO will ensure SSH, or a functionally similar utility, is used to encrypt all communications by all personnel, except from the system console to the system console device. The sole exception is for systems in the demilitarized zone (DMZ).*
- *(G575: CAT II) The SA will ensure SSH is configured to work with TCP_WRAPPERS except in cases where the encryption utility can be configured for IP filtering and still display banners before granting access.*
- *(G581: CAT II) The SA will ensure the owner of the /etc/norouter file is root with a group owner of sys and permissions of 400.*
- *(G623: CAT II) The SA will ensure the public instant messaging clients are not installed.*

- *(G625: CAT II) The SA will ensure that instant messaging clients used for an internal or DOD controlled IM application are at the current patch level.*
- *(G627: CAT II) The SA will ensure that peer-to-peer file-sharing applications are not installed unless authorized and documented with the DAA.*
- *(G653: CAT II) The SA will ensure NIS maps are protected through hard-to-guess domain names.*
- *(G667: CAT II) The SA will ensure NIS maps are protected through hard-to-guess domain names.*
- *(G681: CAT II) The SA will ensure methods used to check file integrity will notify the SA and the IAO via email if a security breach or a suspected security breach is discovered.*
- *(G687: CAT II) The SA will ensure an access control program (e.g., TCP_WRAPPERS) hosts.deny and hosts.allow files (or equivalent) are used to grant or deny system access to specific hosts.*
- *(SO03: CAT II) The SA will ensure the nosuid option is configured in the /etc/rmmount.conf file.*
- *(SO33: CAT II) The SA will ensure the EEPROM password is set using STIG standards.*
- *(SO35: CAT III) The SA will ensure the EEPROM password is not the same as the root password.*
- *(SO45: CAT I) The SA will ensure only root has the gid of 0 (root).*
- *(IRIX05: CAT II) The SA will ensure the Command (PROM) Monitor is password protected.*
- *(IRIX07: CAT II) The SA will ensure the Command (PROM) Monitor password is set using STIG standards.*
- *(IRIX09: CAT III) The SA will ensure the Command (PROM) Monitor password is not the same as the root password.*
- *(L017: CAT I) The SA will encrypt the LILO boot loader password.*
- *(L061: CAT I) The SA will ensure the insecure option is not set.*
- *(L069: CAT II) The SA will ensure the group owner of the /etc/securetty file is root, sys, or bin.*
- *(L071: CAT II) The SA will ensure the owner of the /etc/securetty file is root.*

- *(L073: CAT II) The SA will ensure the /etc/securetty file has permissions of 640, or more restrictive.*

- *(L075: CAT II) The SA will ensure RealPlayer version 8 is removed from SuSE 9.1 and SuSE Linux Desktop 1.0.*

Appendix Changes

- Appendix, Standard Security File Template

  - Deleted this appendix. This appendix contained obsolete data, also, too difficult to ensure accurate data for the reviewer and user community. Checks are contained throughout this *STIG* to properly and more accurately check for required file ownership and permissions for system files.

- Appendix, Require Audit Flag Settings

  - Deleted this appendix. This data will be captured in the *UNIX Checklist* to allow for ongoing updates as systems change and functionality is enhanced.

- Appendix, DISA Field Security Operation ESM/ITA Directives Acquisition Instructions

  - Deleted this appendix. This appendix is no longer valid.

- Appendix, Install Checklist – Creating New Systems

  - Deleted this appendix. This contains incomplete information. The *UNIX Checklist* is a better resource for obtaining up-to-date technical guidance.

- Appendix, Acknowledgement of Risk Letter For Data Transfer Interface Userids

  - Updated this appendix to provide a Acknowledgment of Risk Letter Template. This is provided for FTP and Telnet uses.

- Appendix, UNIX IAVA Detection Procedures and Summary

  - Deleted this appendix.

- Appendix, Install Checklist – Creating New Systems

  - Deleted this appendix. This appendix did not take into consideration all platforms of UNIX as well as all security requirements. This *STIG* and the *UNIX Checklist* in its entirety is a more accurate and complete source for UNIX security requirements for new systems.

- Appendix, List of Accronyms
  - Updated this appendix to accurately reflect the acronyms contained within this *STIG*.

1. INTRODUCTION

This *STIG* is intended to provide configuration guidance and is **not** to be construed as an endorsement or approval for the use of any product. Per the *Department of Defense Directive (DODD) 8500.1*, "All COTS IA or IA-enabled IT hardware, firmware, and software components or products incorporated into DOD information systems must comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11, reference (w). Such products must be satisfactorily evaluated and validated either prior to purchase or as a condition of purchase (i.e., vendors will warrant, in their responses to a solicitation and as a condition of the contract, that the vendor's products will be satisfactorily validated within a period-of-time specified in the solicitation and the contract). Purchase contracts shall specify that product validation will be maintained for updated versions or modifications by subsequent evaluation or through participation in the National Information Assurance Partnership (NIAP), Assurance Maintenance Program." For exceptions to this policy, please see the updated NSTISSP 11 (July 2003) for specific guidance on Exemptions and Deferred Compliance.

1.1 Background

Department of Defense Directive (DODD) 8500.1 establishes policy and assigns responsibilities to the Defense Information Systems Agency (DISA) to develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the National Security Agency (NSA). Paragraph 4.18 of the 8500.1 states, "All IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines." DISA Field Security Operations (FSO) develops the guidelines, which are called Security Technical Implementation Guides.

Tests and studies indicate the following vulnerabilities and system resources (in descending order of ease of exploitation) account for 90 percent of all successful system attacks:

- Electronic mail daemons
- Domain Name System/Service
- Denial of service
- Broadcast messages
- Remote system status calls
- Personal computer (PC) filesystem
- Anonymous file transfer protocol (ftp)
- Network filesystem
- Password files
- Standard ftp

Even the Secret Internet Protocol Router Network (SIPRNet) system vulnerabilities generally follow this pattern, with mail systems and remote command execution being, by far, the most easily and frequently exploited areas.

Additionally, the results of initial system security reviews performed by the DOD Inspector General (DODIG) at DISA sites revealed significant security vulnerability findings. The number of findings caused the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASDC3I) to create a task force charged with identifying and helping to resolve security vulnerabilities at the sites.

It should be noted that FSO Support for the STIGs, Checklists, and Tools is only available to DOD Customers.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing sensitive information.

1.3 Scope

This document is a requirement for all DOD administered systems and all systems connected to DOD networks. This document provides requirements to limit the security vulnerabilities for a UNIX system. These requirements and the steps required to mitigate security vulnerabilities are discussed. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls in a UNIX environment.

DOD customers use several different UNIX platforms that support different versions of UNIX. All UNIX systems share some common characteristics, but at the same time, implement features differently, do not implement all the same features, or use different methods for implementing some of the same features. This document provides security requirements for all common flavors of UNIX.

The Center of Internet Security (CIS) provides several UNIX/Linux benchmarks that contain industry standard security guidance, which may additionally aid the site in their UNIX/Linux security efforts. These benchmarks can be found at http://www.cisecurity.com.

1.4 Writing Conventions

Throughout this document, statements are written using words such as "**will**" and "**should**." The following paragraphs are intended to clarify how these STIG statements are to be interpreted.

A reference that uses "**will**," indicate mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This makes all "**will**" statements easier to locate and interpret from the context of the topic. The IAO will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy the requirement.

A reference to "**should**" indicates a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs but not in the italicized policy bullets. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

Each file name, directory path, binary, command, or code contructs are in a font of Courier New. This Courier New font will allow the user a visual queue to items that are seen on the UNIX screen and the security requirements related to these items.

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Code Definitions

1.6 DISA Information Assurance Vulnerability Management (IAVM)

The DOD has mandated that all IAVMs are received and acted on by all commands, agencies, and organizations within the DOD. The IAVM process provides notification of these vulnerability alerts and requires that each of these organizations take appropriate actions in accordance with the issued alert. IAVM notifications can be accessed at the Joint Task Force - Global Network Operations (JTF-GNO) web site: http://www.cert.mil.

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information. The NIPRNet URL for the IASE site is: http://iase.disa.mil/.

1.8 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to **fso_spt@disa.mil**. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

2. UNIX OVERVIEW AND SITE INFORMATION

2.1 Organizational Relationships

Organizational relationships play a significant role in providing for the security of the environment. The site must provide a robust and secure environment that protects the software environment from unauthorized access. This includes the protection of system-level resources (i.e., database systems, applications, and other utilities) used by the DOD user community. Data owners must define access requirements for their resources (i.e., actual databases, master files, and interactive transactions). Data owners are responsible for providing an access matrix that reflects subjects (processes and authorized personnel) and their access to resources (databases and applications).

2.2 Security Administration

Security administration is accomplished through the ongoing efforts of a number of personnel. The SM is the principal advisor to the site Commander/Director for the administration and management of the overall site security program. The IAM is responsible for the information assurance program of a DOD information system or organization. The IAO is responsible for implementing security requirements and ensuring the operational Information Assurance (IA) posture is maintained for a DOD information system or organization. The IAO is responsible to the IAM. The SA is responsible for the operational readiness and secure state of a computer system. The SA assists the IAO with implementing security directives in the operations environment and reports to the IAO.

2.3 Processing Environment

The UNIX operating system can provide a Class C2 trusted computing base. There are many objectives and goals to be considered when securing a UNIX operating system. When configuring UNIX operating system security, consider these critical principals of security known as the Confidentiality, Integrity, and Availability (CIA) triad:

- Confidentiality
- Integrity
- Availability

In addition to incorporating security controls that relate to the CIA triad, there are three additional security features that directly affect CIA and aid the overall site security program:

- Access control
- Auditing
- Backups

Access controls protect the systems and resources from unauthorized access and in some implementations can determine levels of authorizations. Access controls can include physical access restrictions to ensure only authorized personnel may access system equipment and the environments on which these systems reside. Access controls may also include system level access controls. System level access controls restrict access to system resources and objects, as well as restricting the capabilities of subjects to communicate with other subjects.

Auditing tools can track system activities to warn an SA of suspicious activity, allow the SA to understand the types of access that took place, identify a security breach, and aid in the research of the breach.

Backups are performed with prevention and recovery in mind. This includes, but is not limited to, the prevention of data loss and the loss of availability to data and resources. A daily backup of all changeable data and the proper storage of the data is invaluable in restoring data once a compromise has been detected and traced to the time it first occurred. Without these continual and consistent backups, recovery procedures are not reliable. Backups are also the only way Continuity of Operations Plan (COOP) can be implemented during catastrophe, natural disaster, hardware failures, and other circumstances. In all cases, the quality and depth of backups and the security of backup storage will have a direct impact on the quality and depth of restorative operations and COOP. It is the only path back to confidentiality, integrity, and availability of data once there has been a compromise, a natural disaster, or a catastrophe.

2.4 UNIX Security Design

UNIX generally recognizes three user types: root (also referred to as the superuser), privileged users, and other users. Root is normally, but not necessarily, granted global privileges by the operating system. Role Based Access Control (RBAC) may also be implemented within most UNIX systems. RBAC allows for the delegation of administrative tasks, eliminating or reducing the need for superuser privileges granted to the root user and the root user alone.

Files are assigned access permissions with standard UNIX permissions or additionally with access control lists (ACLs). The sometimes cumbersome and restrictive nature of the standard UNIX file permissions is not always suitable for certain tasks. ACLs provide a greater degree of file access control and a more granular level of file protection, allowing certain privileges to either specific users or specific groups of users. This granular level of file protection provides more flexibility for ensuring file and directory access restrictions.

The standard UNIX file protection provides read, write, and execute permissions for three classes of users. These classes of users are owner, group, and other. Each class may be granted access to a file using any combination of the following three permissions:

- Read
- Write
- Execute

The permission of "read" allows for the ability to read a file or list the contents of a directory. The permission of "write," allows for the ability to edit a file, or add or delete a directory entry. The permission of execute, allows for the ability to execute an executable file or access a directory. In the event a directory is required to allow all users permission to "write" to this directory, such as the case of public directories (e.g., `/tmp`), the sticky bit must be set. This sticky bit protects the files within this directory by preventing a user from deleting other users' files also located in this public directory. When a sticky bit has been set on a directory, the owner of the file, owner of the directory, or root, can only delete a file.

2.5 Integrity

Computer information system integrity encompasses the accuracy, reliability, and correctness of a system. The system includes the hardware, software, data, and communications. The system must be able to process data as expected, maintain and ensure correctness of data, and securely process communications to and from the system.

Sites achieve UNIX system and data integrity by managing the complete system environment. Proper security and system management protects system hardware, software, applications, and data from unauthorized access and improper modification and leads to the secure operation of UNIX systems. The integrity of a system is most vulnerable to malicious intrusion before systems have been completely configured for secure operation. Newly built or configured systems increase the risk of a data integrity compromise upon connection to a production network if the system is not completely configured for secure operation.

2.5.1 Hardware Integrity

Hardware resources include central processing units (CPUs), disk drives, terminals, workstations, printers, as well as many other hardware components. Incorrectly installed, operated, or maintained hardware creates security vulnerabilities.

Controlling access to hardware resources is essential. Physical access control reduces the risk of theft, damage, and unauthorized access. Specific installation guidelines apply to classified equipment.

The operating environment must be capable of protecting the integrity of the hardware through physical means. The following sections define the hardware integrity requirements.

2.5.1.1 System Equipment

The UNIX operating system resides on, stores information on, and is accessed by a number of different devices including the hardware resources discussed in *Section 2.5.1, Hardware Integrity*. System equipment will be protected from physical security countermeasures, as well as unauthorized access to the operating system via physical access to the system equipment.

Unauthorized access to the operating system may be gained via physical access by booting the server to a single-user mode. With basic UNIX knowledge and physical access to the CPU, the system can be booted to single-user or maintenance mode and in turn, root privileges will be gained. In single-user mode, the standard UNIX Identification and Authentication (I&A) process is not enabled. Sites will configure all systems that support the requirement for single-user passwords to enable and configure that feature. Systems that cannot be configured to require a single-user password are to be documented with the IAO and located in a restricted and controlled access area accessible only by SAs. Additionally, secure the console and other hardware for such systems in a restricted and controlled access area to prevent accidental or malicious access.

To provide minimal physical protection for other systems and certain peripherals, locate them in a controlled access area that requires positive identification (e.g., a swipe card) for entry. All systems will be furnished with a maintenance log. Enter all single-user and maintenance actions in the maintenance log to provide a history of actions that may be needed for possible recovery operations.

- *(G001: CAT II) The IAO and SA will ensure all UNIX hosts are configured to require a password for access to single-user and maintenance modes.*

- *(G003: CAT II) The SA will ensure any UNIX hosts that cannot be configured to require a password when booted to single-user mode is to be justified and documented with the IAO.*

- *(G005: CAT II) The SA will ensure any UNIX hosts that cannot be configured to require a password when booted to single-user mode is to be located in a controlled access area accessible only by SAs.*

- *(G007: CAT II) The SA will ensure all UNIX system equipment (e.g., workstations, terminals, etc.) will be located in a controlled access area.*

- *(G009: CAT I) The IAO will ensure the operating system is a supported release.*

2.5.2 Public Domain Software

DOD has clarified policy on the use of open source software to take advantage of the capabilities available in the Open Source community, as long as certain prerequisites are met. DOD no longer requires that operating system software be obtained through a valid vendor channel and have a formal support path, if the source code for the operating system is publicly available for review. Public domain software may be used when there is an operational requirement that compels the use of the software. The responsible DAA accesses and accepts the risk of integrated public domain software.

DOD CIO Memo, Open Source Software (OSS) in Department of Defense (DOD), 28 May 2003:

> "DOD Components acquiring, using or developing OSS must ensure that the OSS complies with the same DOD policies that govern Commercial-Off-The-Shelf (COTS) and Government-Off-The Shelf (GOTS) software. This includes, but is not limited to, the requirements that all information assurance (IA) or IA-enabled IT hardware, firmware and software components or products incorporated into DOD information systems whether acquired or originated within DOD;
>
> - Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and;
>
> - Be configured in accordance with DOD-approved security and configuration guidelines at http://iase.disa.mil/ and http://www.nas.gov/."

Linux is acceptable based on the availability of source code, in some instances, and the support and guarantee of the vendor (e.g., Red Hat) and the support and guarantee of vendors who incorporate the software in their common release. Please additionally note that any UNIX based operating system in use in a DOD environment is subject to all relevant UNIX security requirements and must be capable of STIG compliance as verified by a System Readiness Review (SRR).

2.5.3 Data Integrity

DISAI 630-230-19 provides the concepts to be used in evaluating the data integrity requirements supporting application data. This *STIG* is not intended to address data-level integrity in detail, but to provide techniques that can be used to help ensure security of the data residing on a UNIX platform.

Filesystem access and security controls play a critical role in maintaining the integrity of UNIX systems. Several key areas of control requirements are discussed in the following sections.

2.5.3.1 File Integrity

Maintaining file integrity is a key factor in the protection of UNIX systems. Monitoring the access and modification of critical files (e.g., system files and libraries, application files, device files, etc.,) is a major component of ensuring file integrity. A baseline is a database that contains a snapshot of the system after it has been fully loaded with operating system files, applications, and users. Baseline control consists of comparing a current system snapshot with the original system snapshot. The purpose of maintaining and checking a system baseline is to detect unauthorized system changes. Unauthorized changes may indicate system compromise and, if detected, could prevent serious damage. A baseline consists of files that change infrequently in terms of size, access permissions, modification times, checksums, etc. They are most often found in the system directories but could be in other locations. It would be a mistake to try to

maintain a baseline of user files and/or temporary files (i.e., files located in the `/tmp` directory) since these constantly change.

The integrity of sensitive system files will be checked at least weekly against a known baseline of these files using a baseline checking utility. A listing and description of some baseline checking tools are located in *Section 6, UNIX Security Tools*. Whatever is used, it must notify the IAO/SA of any unexpected changes. The SA and IAO will investigate any anomalies and decide if an actual file integrity breach has occurred. The system date and time-of-day can be a key forensic factor in detecting and tracking file compromises. Due to the great importance of the accuracy of the system clock and date setting, the SA will ensure the ongoing accuracy of the system clock and date. The accuracy of a system clock can be considered accurate if within 60 seconds of an authoritative DOD approved time-server. Authoritative DOD approved time-server sources for the NIPRNet can be found at http://tycho.usno.navy.mil/ntp.html. *Section 6, UNIX Security Tools,* includes discussion as well as additional security software requirements.

The file system integrity tool will take a baseline of all files, or a specific subset of files, to include cryptographic hashes of files in the baseline. The tool must be able to compare the existing baseline of the system against the current state of the system, so that unauthorized modification of the operating system can be detected.

The SA, under the direction of the IAO, is responsible for creating, checking, and maintaining a current system baseline. The IAO is responsible for verifying the system baseline. The IAM is responsible for setting overall policy for system baseline creation and maintenance.

A UNIX filesystem contains files and directories. A special number called an inode represents these files and directories. The inode allows the UNIX operating system to create and keep track of filesystems. The inode contains information that includes its location, size, type, and number of directory entries linked to the file. The inodes store all information about a filesystem entry except its name. This information makes it possible to collect all the information about a file when it is needed.

The baseline database will be backed up on write-protected media and checked against the current baseline while the system is in single-user mode. Note the baseline changes whenever a change is made to the system. Changes include adding patches and packages. A new system baseline will be executed after every software change and after changes to system directories and files are applied.

- *(G011: CAT II) The SA will create and maintain a system baseline (all device files, sgid and suid file, and system libraries and binaries), to include cryptographic hashes of files in the baseline.*

- *(G013: CAT II) The SA will maintain all baseline backups on write-protected media.*

- *(G015: CAT II) The SA will execute a new system baseline after every software change.*

- *(G017: CAT II) The SA will execute a new system baseline after changes to system directories and files are applied.*

- *(G019: CAT II) The SA will ensure the accuracy of the system clock and date.*

- *(G021: CAT I) The SA will ensure the outside network time-server will be from an authoritative U.S. DOD source for both the NIPRNet and the SIPRNet.*

This page is intentionally left blank.

3. DISCRETIONARY ACCESS CONTROL AND GENERAL SECURITY

This section discusses discretionary access control (DAC), overall general UNIX security measures, and the I&A criteria necessary to ensure access to system resources is effectively managed and controlled for the UNIX system. In this sense, it is also discussing confidentiality, which consists of assurance that information is not disclosed to unauthorized persons, processes, or devices. This entails incorporating the concept of least privilege. Least privilege states that users have only the authority to access those resources necessary to perform their required functions. DAC places a large part of the responsibility for data confidentially, integrity, and availability directly into the data owners hands by delegating to the owner the ability to determine who can access the data and how it is accessed (e.g., read, write, delete). This *STIG* attempts to provide secure methods of accomplishing DAC and other operations, while still protecting the data owner, the data user, and the platform's operating system.

3.1 User Account Controls

C2 compatibility requires individual user accountability. This precludes the use of shared accounts (i.e., accounts where multiple users are allowed to log on directly to the same account). Applications may require that a specific account (e.g., oracle) be used for certain administrative tasks. The user is required to log on with that user's account name and `su -` to the application account. That action retains the individual accountability (through audit files) that C2 requires. If there is an application account (e.g., oracle) that requires the account to be shared, this will be justified and documented with the IAO. If there is a vendor requirement for logging directly into an account, the IAO will obtain justification and documentation from the vendor that states the necessity and justification.

- *(G023: CAT II) The SA will ensure any special purpose accounts or applications requiring a shared account are documented with the IAO. Documentation will include a statement from the SA or application developer, where applicable, stating the absolute necessity of and justification for the shared account.*

- *(G025: CAT II) The IAO will ensure shared account logons are accomplished by invoking the `su -` (switch user) command from the individual user's UNIX session; the shared account will not be logged into directly.*

3.1.1 Interactive Users

DOD directives require unique identification for each system user. Authorized users should be granted access only to the resources needed to accomplish their mission. A user is either an individual or an executing process/task that accesses a computer resource. Each user will be identified with an account name and a corresponding user identification (uid) number. The uids and group identification (gid) numbers are assigned according to the following scheme:

- UNIX
  - uids
    - 0 – 99 Reserved for system account uids.
    - 100 – 999 Generally used for application uids.
    - 1000 – 60000 Generally used for interactive/user uids.
  - gids
    - 0 – 99 Reserved for system account gids.
- Linux
  - uids
    - 0 – 499 Reserved for system account uids.
    - 500 – 999 Generally used for application uids.
    - 1000 – 60000 Generally used for interactive/user uids.
  - gids
    - 0 – 499 Reserved for system account gids.

NOTE: Debian application uids and user ids are 1000 – 29999.

C2 security requires all users accomplish I&A to a computing system with a minimum of a legitimate, authenticated account name and password pair before access to computing resources is granted. *DISAI 630-230-19* defines the requirements for user access. The IAO controls access to UNIX resources by authorizing the functionality of user accounts. The SA will assign users and applications a uid based on the above detailed guidance. Systems reserve the first 99 (499 for Linux) uids and gids for system use.

Groups are collections of users with common resource requirements. Users are given resource access by the rights provided to a group. All users will belong to at least one group. Systems reserve gids 99 (499 for Linux) and below for system use. Therefore, the SA will assign users and applications a gid based on the above detailed guidance. An example of a valid situation to add a user to a group with a gid of less than 100 would be the System Administrators on Solaris. System Administrators need to be a member of the sysadmin group (e.g., gid 14) to allow for use of the Admintool. There is no technical justification for the use of the Solaris staff group (i.e., gid 10). All gids that appear in the `passwd` file will be defined in the `group` file in order to maintain order and to maintain the integrity of the `passwd` file and `group` file.

Examples of valid situations where a user account has a gid of less than 100;

- Solaris
  - gid 10 (staff) — Not recommended, but allowable. Requires documentation with the IAO.
  - gid 14 (sysadmin) — System Administrators need to be a member of the sysadmin group (i.e., gid 14) to allow for use of the Admintool. Requires documentation with the IAO.
- HPUX
  - gid 20 (users) — Not recommended, but allowable. Requires documentation with the IAO.

- *(G027: CAT III) The SA will ensure each user is assigned a unique account name.*
- *(G029: CAT II) The SA will ensure each user is assigned a unique uid.*
- *(G031: CAT II) The SA will ensure uids 0 – 99 (0 – 499 for Linux) are reserved for system accounts.*
- *(G033: CAT II) The SA will ensure gids 0 – 99 (0 – 499 for Linux) are reserved for system accounts. If used, the exceptions (detailed above) must be documented with the IAO.*
- *(G035: CAT IV) The SA will ensure each group referenced in the* `/etc/passwd` *file will be defined in the* `/etc/group` *file.*

3.1.2 Logon Warning Banner

Criminal court cases involving unauthorized access to official government computer systems has prompted the need for a logon warning banner to be presented to anyone accessing a government computer system. A compressed version (subset) may be used as long as the criteria below are met. The following sample is provided by the *CJCM 6510.01 (Final).*

> This is a Department of Defense computer system. This computer system, including all related equipment, networks, and network devices (specifically including internet access), are provided only for authorized U.S. Government use. DOD computer systems may be monitored for all lawful purposes, including ensuring their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DOD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system, may be monitored.

> Use of this DOD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

A compressed version (subset) may be used as long as the criteria below are met:

- The system is a DOD system.
- The system is subject to monitoring.
- Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.
- Use of the system constitutes consent to monitoring.

- *(G037: CAT II) The SA will ensure a logon-warning banner is displayed on all devices and sessions that allow application or command-level access prior to logon attempts.*

- *(G039: CAT II) The IAO will ensure the Legal Notice Logon Warning Banner includes the four points outlined in the 16 January 1997 message from Assistant Secretary of Defense, Subject: Policy on DOD Electronic Notice and Consent Banner. All DOD AISs will display, as a minimum, an electronic "logon notice and consent banner" that advises users of the following principles:*
  - *The system is a DOD system.*
  - *The system is subject to monitoring.*
  - *Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.*
  - *Use of the system constitutes consent to monitoring.*

3.1.3 Account Access

Many computer compromises occur as the result of account name and password guessing. This is generally done with an automated script that uses repeated logon attempts until the correct account and password are guessed. Logon and logout logs for users, as well as root, account locking, retry delays, and session disconnect are effective methods of controlling potentially malicious account access. The SA will properly configure these methods to control unauthorized account access. Most systems do support account lockout, while some systems will disconnect the session after three consecutive failed logon attempts. After three failed logon attempts, the account will be locked. After three to five failed logon attempts, the session will be disconnected; three is the preferred amount of attempts. However, in consideration of different system support, which is beyond the configuration control, and cannot be modified, some systems do support session disconnect after three failed logon attempts, some support session disconnect after five failed attempts, and some are configurable for the number of failed attempts to allow. The different system support will be detailed in the *UNIX Checklist*; this will allow for continual updates as the UNIX flavors enhance the operating system.

- *(G041: CAT II) The SA will ensure all logon attempts (both successful and unsuccessful) are logged to a system log file.*

- *(G043: CAT II) The SA will ensure, after three consecutive failed logon attempts for an account, the account will be locked until the SA unlocks the account.*

- *(G045: CAT II) The SA will ensure all systems are configured to provide session disconnect after three consecutive failed logon attempts on a session have been reached. Some systems will only support a minimum of five; this is acceptable on that occasion.*

- *(G047: CAT II) The SA will ensure the logon delay between logon prompts after a failed logon is set to at least four seconds.*

3.1.4 Inactivity Timeout/Locking

When a user is logged on to a UNIX system, the system is susceptible to alteration or damage. A user may become busy or distracted and inadvertently leave a logon session. Such idle sessions leave the UNIX system vulnerable to unauthorized user exploitation. Users will ensure they log out when they are finished with a session. When a workstation is left unattended, users will ensure sessions are locked and not accessible without I&A or the user will log out. There are also additional options that may be employed to ensure a session is not left unattended, such as token cards. Token cards are removed from a client when leaving a console and the token card is then used for access to the console upon return. Sessions/terminals will be logged out or locked after 15 minutes of inactivity. Screen lock programs can be configured to activate if terminals are idle for a specified period. Shells (e.g., `sh`, `ksh`, etc.) also contain variables that can be set to terminate logon sessions after a specified period of inactivity. If a screen lock device is available, it should be able to be invoked by the user when the user wishes to leave the terminal unattended. Most terminals provide screen lockout, as opposed to session termination. Some terminals require continuous displays, such as network management terminals, and may be

exempt from the requirement as long as they are located in a restricted access area and fully justified and documented with the IAO.

- *(G049: CAT III) The SA will ensure all terminals/consoles requiring a continuous display are physically located in a restricted access area.*

- *(G051: CAT II) The SA will ensure applications requiring continuous, real-time screen display (i.e., network management products) are exempt from the inactivity requirement provided the following requirements are met:*

  - *The logon session is not a root session.*
  - *The inactivity exemption is justified and documented with the IAO.*
  - *The display station (i.e., keyboard, CRT) is located in a controlled access area.*

- *(G053: CAT II) The SA will configure systems to log out interactive processes (i.e., terminal sessions, ssh sessions, etc.,) after 15 minutes of inactivity or ensure a password protected screen lock mechanism is used and is set to lock the screen after 15 minutes of inactivity.*

3.2 Password Controls

UNIX operating systems allow specification of a password. The following guidelines will be used for password creation.

3.2.1 Password Guidelines

Apply the required information assurance controls for the Mission Assurance Category (MAC) and Confidentiality Level in accordance with *Enclosure 4, DODI 8500.2*. Modern UNIX systems accomplish this by encrypting passwords and placing them into a protected file that is separate from, and more secure than, the `/etc/passwd` file. Implementation of the password protection scheme is listed below and is dependent on the flavor of UNIX used:

1. In most System V, Solaris, Linux, and IRIX this is implemented in the `/etc/shadow` file.

2. In HP-UX 10.X and 11.X systems, running in secure mode, this is implemented in the `/tcb/files/auth` directory. This directory consists of a series of sub-directories (a-z, for instance) named for the first letter of the account name. Each directory contains a password record for each user whose account begins with that letter.

3. In AIX systems, this is implemented in the `/etc/security/passwd` file.

Users must take precautions to protect passwords by choosing them wisely. Studies have shown that users who are allowed to choose their own passwords are more likely to remember them. Passwords so complex or obscure that they require recording to remember introduce the hazard of becoming accessible to unauthorized persons. A good password would be a pronounceable non-word to help users remember, but not too complicated to cause the user to document the password.

NOTE: Some systems will not allow the '#' and/or the '@' sign in passwords and certainly not in the account name.

There are several additional password guidelines to be configured, which provide additional system and user account protection. These include ensuring passwords are changed every 90 days for users as well as root. These password guidelines are to be configured for each individual user account as well as the global system password configuration file(s). Accounts created for and used by non-interactive/automated processing are subject to special consideration. These accounts may be used for a variety of functions such as activity log storage by remote or local devices, unattended database maintenance batch jobs, etc. These accounts will not be shared with interactive database users. Passwords for non-interactive/automated processing accounts will be changed at least once a year and anytime an application administrator is reassigned. When an individial with access to the root password is reassigned, the root password will be changed. Accounts will be locked after 35 days of inactivity. Accounts will be locked by making the default shell `/bin/false`, `/usr/bin/false`, `/sbin/false`, `/sbin/nologin`, or `/dev/null`, and/or by locking the password. Passwords will not be reused within the last ten changes. Access to the root account is to be limited to security and administrative users who require such access, these users are to be documented with the IAO as having such access.

- *(G055: CAT II) The SA will ensure passwords are not changed more than once a day.*
- *(G057: CAT I) The SA will ensure each account in the* `/etc/passwd` *file has a password assigned or is disabled in the password, shadow, or equivalent, file by disabling the password and/or by assigning a false shell in the password file.*
- *(G059: CAT II) The IAO will ensure all passwords contain a minimum of eight characters.*
- *(G061: CAT II) The IAO will ensure passwords include at least two alphabetic characters, one of which must be capitalized.*
- *(G063: CAT II) The IAO will ensure passwords include at least one numeric character.*
- *(G065: CAT II) The IAO will ensure passwords contain at least one special character, avoid '#' and '@'.*
- *(G067: CAT II) The IAO will ensure passwords will not contain information such as names, telephone numbers, account names, dictionary words, etc.*

- *(G069: CAT II) The IAO will ensure passwords contain no consecutively repeating characters.*
- *(G071: CAT II) The SA will ensure passwords are changed at least every 90 days.*
- *(G073: CAT II) The SA will ensure the root password is changed at least every 90 days.*
- *(G075: CAT II) The SA will ensure passwords for non-interactive/automated processing accounts will be changed at least once a year and anytime an application administrator is reassigned.*
- *(G077: CAT II) The SA will ensure passwords expire after 35 days of inactivity.*
- *(G079: CAT I) The SA will ensure easily guessed passwords are not used.*
- *(G081: CAT II) The SA will ensure passwords will not be reused within the last ten changes.*
- *(G083: CAT II) The SA will ensure the system global password configuration files are configured per password requirements.*
- *(G085: CAT II) The SA will ensure access to the root account is limited to security and administrative users who require such access. These users are to be documented with the IAO as having such access.*
- *(G087: CAT III) The IAO or SA will ensure the root password will be changed whenever an individual with access to the root password is reassigned.*

3.3 Root Account

The root account is used to accomplish system administrative functions. The system uses this account to run privileged programs. Because root enjoys access to all files and programs, root has no security constraints.

In most flavors of UNIX, by default, the root home directory is '/' which is readable by all UNIX users. In Linux, by default, the root home directory is `/root`. The root home directory will be in a directory other than '/' to afford the root startup and work files the same protection as is afforded to all other users. Sun's `vipw` (an old, manual method of altering the `passwd` file which has been superceded by the `admintool`) will not work correctly with this change. Using the Graphical User Interface (GUI), `admintool` - the recommended method, is not affected.

Sites usually designate one or more primary and alternate SAs requiring root access. Sharing accounts and/or the root account and password is a breach of the C2-level security requirement for individual I&A and defeats the audit mechanism. The security breach is eliminated when all SAs and users log on using their individual account I&A; then, use the `su -` command to switch to a privileged account, especially if it is the root account. Use of the `su -` command and the `sulog` file, along with system auditing, gives the ability to identify use of authorized shared accounts (particularly the root account) and to audit those actions in an irrefutable manner. When using the `su` command, the `su` command should be called using the full path of the utility as well the **'-'** sign is to be used (e.g., `/bin/su -`). Using the full path to the utility ensures the correct binary is called. Using the **'-'** sign will ensure the privileged and/or root's environment is to be used when a user switches to the privileged user and/or root.

The root account will not have a directory in the search path that is group and/or world writable or search in the current working directory. Current working directories or group and/or world writable directories that root searches allows for the modification of current binaries or addition of trojanized binaries which root would execute when searching for a binary to execute. A **'.'**, **'::'** or, **':'** as the last element of a PATH definition represents the current directory.

Accounts that `su –` to the root account will be bound by the same restrictions of the root account. They will log on to their named accounts. They will invoke the `su –` command to reach root, or the root role they have been assigned, if necessary. Their `PATH` will be the same as the root `PATH` once the command is completed. In any case, their personal `PATH` environment will be bound by the same restrictions as the root `PATH` environment. This restriction protects against the root capable account accidentally using `su` instead of `su –`, and dragging a default environment with an incorrect `PATH` variable along with it, as well as the obvious potential for compromise. Users with root capabilities should not be identified as such in the comment field of the `passwd` file to avoid clarifying potential targets for malicious users and/or intruders.

The only user with a uid of zero (0) will be root, as the uid of 0 allows superuser privileges. If another uid of zero (0) is in the password file, it may be an indication of system compromise. The smtp account that is distributed with Solaris 7 and earlier comes configured with a uid of zero (0). This uid is not necessary with the Solaris configurations. The smtp account uid will be changed (the uid of 6 is recommended), or the account deleted entirely.

The root account default shell will be located in `/sbin` or `/bin` if `/usr` has been partitioned (i.e., is not a part of the '/' partition). This is to maintain a consistent environment for root across platforms, systems, and sites. In the event `/usr` is partitioned, this also ensures that root will have a shell when in single user or repair/maintenance modes, since `/sbin` is in the root filesystem and, for instance, `/usr/bin` is not in the root filesystem. The SA may invoke a different shell from the command line, after logging on and switching user to root (`/bin/su -`), by invoking the alternate shell and sourcing the necessary files.

- *(G089: CAT II) The SA will ensure only root has a uid of 0.*

- *(G091: CAT IV) The SA will ensure root is assigned a home directory other than '/' (e.g., `/roothome`).*

- *(G093: CAT II) The SA will ensure the root account home directory (other than '/') has permissions of 700. Do not change the permissions of the '/' directory to anything other than 0755.*

- *(G095: CAT II) The SA will ensure the root search `PATH` (and the search path of root capable accounts) does not contain* ***'.'****,* ***'::'****, or start or end with a* ***':'****. All are equivalent to '.'.*

- *(G097: CAT II) The SA will ensure root's `PATH` (and the search path of root capable accounts) does not contain directories or files that are world writable.*

- *(G099: CAT II) The SA will ensure root can only log on as root from the system console, and then only when necessary to perform system maintenance.*

- *(G101: CAT I) The SA will ensure the remote console feature is not implemented.*

- *(G103: CAT II) The IAO will enforce users requiring root privileges to log on to their personal account and invoke the `/bin/su -` command to switch user to root.*

- *(G105: CAT II) The SA will ensure successful and unsuccessful root logon and logout attempts are recorded in a system log.*

- *(G107: CAT II) The SA will ensure successful and useccessful switch user (`su -`) attempts are recorded in a system log.*

- *(G109: CAT III) The SA will ensure the root shell is not located in `/usr` if `/usr` is partitioned.*

3.3.1 Encrypted Root Access

Information, including passwords, is normally passed in clear text form over the network whenever a user accesses a remote system. If a user accesses the root account (using `/bin/su -`, for instance), the password is passed in clear text form and is subject to interception and malicious misuse. This is true for people who have root capable accounts who leave their personal password in the clear and open to malicious interception.

To protect against password and sensitive data interception, the IAO will require that each system accessed remotely by a privileged user enforce enhanced I&A with encryption. Password and data encryption will allow the root password and sensitive data to be passed over the network with a level of assurance that it will not be intercepted in a usable form. The use of SSH Tectia, OpenSSH, F-Secure, Reflection for Secure IT, or similar programs are some methods for accomplishing this. All systems that are accessed remotely using the root password (or any other privileged account password) will use a password and data encryption for that connection.

Secure Shell (SSH) gives the option to log on remotely as root even when the system has otherwise been configured to disallow direct logon as root. Ensure this feature is disabled in SSH in order to protect the audit trail. SSH also allows `.shosts` (the same as `.rhosts` but used by SSH). These features are not to be used unless the feature is operationally necessary and is documented with the IAO. Refer to *Section 3.10, Trusted System/User Access Control Files* and *Section 4.15, Secure Shell (SSH) and Equivalents*, for guidance on the use of `.rhosts` and `.shosts`.

- *(G111: CAT II) The IAO will require strong I&A, with encryption for password and data, for all remote accesses (access from other than the system console) by the root account.*

- *(G113: CAT II) The SA will configure the encryption program for direct root access only from the system console.*

3.4 Vendor Recommended and Required Patches

Maintaining the security of a UNIX system requires frequent reviews of security bulletins. Many security bulletins and IAVM notifications mandate the installation of software patches to overcome noted security vulnerabilities. The SA will be responsible for installing all such patches on a timely basis. The IAO will ensure the vulnerabilities have been remedied. FSO guidelines for remediation, including IAVMs are as follows:

Remediation Guidelines;

- Apply the applicable patch or upgrade to required software release, or remove the binary/application to remediate the finding.

- Or, the vulnerable binary may be renamed and the permissions modified to 000 to downgrade the finding, for example a CAT I finding may be downgraded to a CAT II.

SAs and IAOs will regularly check OS vendor web sites for information on new vendor recommended and security patches that are applicable to their site. All applicable vendor recommended and security patches will be applied to the system. A patch is deemed applicable if the product is installed, even it is not used or disabled.

- *(G115: CAT II) The SA will ensure vendor recommended and required security patches are applied.*

3.4.1 DOD Patch Repository

DISA maintains a repository of software patches and hot fixes. This patch server can be accessed at the following location:

NIPRNet - https://patches.csd.disa.mil

3.5 File and Directory Controls

UNIX is a multi-user system. This means that multiple users may be concurrently logged on to a machine, and those users can read and use files belonging to each other if they have been granted permission to do so. The owner of a file, or root, can grant access permissions to a file by changing the permission bits. However, no user will possess a more permissive access to a file than the owner does. This is referred to as uneven file permissions. An example is the world having write permission to a file when the group owner is not granted write permission also. The only instance where uneven file permissions will be allowed is in the World Wide Web (WWW) file server directory tree. The uneven file permission allowed will be no more permissive than 460. Every file and directory can be assigned three basic file permissions. These file permissions are as follows:

- Read Allows for the ability to read a file or list the contents of a directory.
- Write Allows for the ability to edit a file or delete a directory entry.
- Execute Allows for the ability to execute an executable file or access a directory.

This group of three permissions is assigned to three classes of users:

- Owner This is usually the creator of the file.
- Group This group of users consists of the users in the file owner's group.
- Other This represents all users on the system.

Files can exist without a discernable owner or group owner by having the uid number and the gid number of a previous user (a user who has been deleted from the system). If a new user is added to the system and assigned the same uid/gid numbers as the previous user, the new user inherits all of the access permissions that previously belonged to the former user. That could mean unauthorized access to sensitive information. For that reason, ownerless files and/or files with no group owner will be deleted or corrected to the proper owner and/or group owner.

Permissions may be assigned by symbolic mode (e.g., rwxr-r--) or absolute mode (e.g., 764).

- 4 Read permission
- 2 Write permission
- 1 Execute permission

The first octal value displays the owner’s permissions. The second octal value displays the group permissions. The third octal value displays the other permissions.

For example, a file with a file access permission of 764 (i.e., rwxr-r--) would grant the following permissions:

- Owner Read, write, and execute (4 + 2 + 1)
- Group Read and write (4 + 2)
- Other Read (4)

There is one change in interpretation for permissions of a directory. In a directory, execute means search. For example, if the above example were a directory, not a file, a directory access permission of 764 would grant the following permissions:

- Owner Read (the contents), write (into), and search (4 + 2 + 1)
- Group Read and write (4 + 2)
- Other Read (4)

The many rules that exist for system file ownership and access permissions must be observed in order to protect system security. All system files will be owned by a system user such as root, sys, bin, lp, etc. Access permissions for system files and directories are set up to allow access by system users and to deny, or strictly limit, access by group owners and the world and will be owned by a system account and group.

A daemon refers to a service or process that runs in the background (or on demand from within `inetd.conf`) and services user requests. The telnet daemon (`telnetd` or `in.telnetd`) is just one example. System commands are utilities that perform system tasks, display system information, etc. Daemons and system commands are not to have group or world write permissions. System log files refer to logs of system activities, such as the `/var/log/syslog` file, the `/var/messages` file, and others. Man pages refer to online manual pages to provide users with an online help mechanism. These log files and man pages are to have permission of 644, or more restrictive to ensure these are not over written or deleted unintentionally or maliciously.

System library files (i.e., files used when compiling and running programs), manual page files (i.e., files that contain instructions for executing commands), and shells (i.e., programs such as `sh` and `csh` that determine the overall user operating environment) require access permissions that limit user access privileges in order to preserve system integrity. Two more special files, the `/etc/passwd` and `/etc/shadow,` or equivalent files, require special protection from malicious intruders in order to protect the account security of every user, including root, applications, and application data.

NIS and NIS+ is a distributed database system that provides a central location for configuring and administering site systems and users. Name service database and map files must be secured to ensure they are not writable by world or unintended users.

- *(G117: CAT II) The SA will ensure there are no uneven file permissions. The exception will be in WWW server directory trees where some files will be allowed a permission of 460.*

- *(G119: CAT II) The SA will ensure all files have a valid owner and group.*
- *(G121: CAT II) The SA will ensure all daemons have permissions of 755, or more restrictive.*
- *(G123: CAT II) The SA will ensure all system commands have permissions of 755, or more restrictive.*
- *(G125: CAT II) The SA will ensure the owner of all system files, programs, and directories is a system account.*
- *(G127: CAT II) The SA will ensure the group owner of all system files, programs, and directories is a system group.*
- *(G129: CAT II) The SA will ensure all system log files have permissions of 644, or more restrictive.*
- *(G131: CAT III) The SA will ensure all manual page files (i.e., files in the man and cat directories) have permissions of 644, or more restrictive.*
- *(G133: CAT II) The SA will ensure all system library files have permissions of 755, or more restrictive.*
- *(G135: CAT II) The SA will ensure the owner of all NIS/NIS+/yp files is root, sys, or bin.*
- *(G137: CAT II) The SA will ensure group owner of all NIS/NIS+/yp files is root, sys, bin, or other group.*
- *(G139: CAT II) The SA will ensure all NIS/NIS+/yp files have permissions of 755, or more restrictive.*
- *(G141: CAT II) The SA will ensure the* `/etc/passwd` *file has permissions of 644, or more restrictive.*
- *(G143: CAT I) The SA will ensure the owner of the* `/etc/passwd` *and* `/etc/shadow` *files (or equivalent) is root.*
- *(G145: CAT II) The SA will ensure the* `/etc/shadow` *file, or equivalent, has permissions of 400.*

3.6 Home Directories

Users will be assigned home directories in the `/etc/passwd` file. A home directory contains a user's files and exists for that user's exclusive use. A user's home directory will be owned by the user and the group owner will be the user's primary group. Home directories will have an initial access permission of 700. DAC allows a user to change the home directory access permissions, but these will never be more permissive than 750, which would allow group read and list access.

- *(G147: CAT IV) The SA will assign every user a home directory in the `/etc/passwd` file.*

- *(G149: CAT IV) The SA will ensure all home directories defined in the `/etc/passwd` file exist.*

- *(G151: CAT II) The SA will ensure user home directories have initial permissions of 700, and never more permissive than 750.*

- *(G153: CAT II) The SA will ensure the user's home directory is owned by the user.*

- *(G155: CAT II) The SA will ensure the gid of an account home directory will be the primary gid of the account (i.e., the one assigned in the `/etc/passwd` file), except in the case of application directories, which will be documented with the IAO.*

3.7 User Files

User files are files owned by a user, except for the possibility of some user local initialization files, which may be owned by root, and maintained by the user in the user's home directory. User files will have an initial access permission of no more permissive than 700 and will never be more permissive than 750. All files in user home directory will be owned by the user with the possible exception of local initialization files that may be owned by root. The SA and the user, as well as application developers, will be responsible for maintaining these requirements.

- *(G157: CAT III) The user, application developers, and the SA will ensure files (excluding a limited set of local initialization files) in user home directory trees will be owned by the user who owns the home directory.*

- *(G159: CAT II) The user, application developers, and the SA will ensure user files will have an initial permission of no more permissive than 700, and never more permissive than 750.*

3.8 Run Control Scripts

Run control scripts are executed by the system and/or kernel when the system is booted. They are also executed (with a different argument such as `stop`) when the system is shut down in an orderly manner. They may also be executed by root at any time. The numbers associated with an `rc` directory name relate to the run level at which the system executes the control scripts. Files in `rc2.d`, for instance, would only be executed when the system is going into run level 2. Run control scripts set parameters for the kernel and start or stop applications and system utilities (such as daemons). Their names and locations are dependent on the system architecture.

Run control scripts normally refer to the files in, and subordinate to, `/etc` that begin with the letters, `rc` or reside in a directory such as `rc0.d`, `rc1.d`, and so on. The number relates to the run level at which they are invoked. The run control scripts are linked between the directories. One startup file may appear five times with different names. Run control scripts may also be linked to other directories but with different names, such as in `/etc/init.d` and `/sbin/init.d`, `/sbin/rc*.d` and `/etc/rc.config.d`, depending on the system.

- *(G161: CAT II) The SA will ensure run control scripts have permissions of 755, or more restrictive.*

- *(G163: CAT II) The SA will ensure run control scripts do not contain '.', '::', or a ':' as the first or last entry in the PATH variable.*

- *(G165: CAT II) The SA will ensure run control scripts files do not have the suid or sgid bit set.*

- *(G167: CAT I) The SA will ensure run control scripts do not execute world writable programs.*

- *(G169: CAT II) The SA will ensure the owner of run control scripts is root.*

- *(G171: CAT II) The SA will ensure the group owner of run control scripts is root, sys, bin, other, or the system default.*

- *(G173: CAT II) The SA will ensure run control scripts only execute programs owned by a privileged uid or an application default.*

3.9 Initialization Files

3.9.1 Global Initialization Files

Global initialization files provide a centralized location to globally distribute and set environment variables and directory paths. The global initialization files are located in the `/etc` directory. Some common global initialization files are `/etc/profile`, `/etc/.login`, `/etc/default/login`, and `/etc/environment` in which global parameters, such as `PATH` variables, may be set each time a user logs on. Global initialization files will be owned by root and will be no more permissive than 644.

Executing the command `mesg -y` opens up the user terminal to writing by all users, the `mesg -y` command will not be executed by a global initialization file, also the global initialization files (e.g., `/etc/profile)` will contain `mesg –n` or `mesg n`.

There are also default user initialization files that are placed in a new user's directory to get them started. Depending on the flavor of UNIX, these are normally located in `/etc/skel` and have names such as `local.cshrc`, `local.login`, `local.profile` (i.e., `dot` files). Default user initialization files will be owned by root or bin and will be no more permissive than 644.

- *(G175: CAT II) The SA will ensure global initialization files have permissions of 644, or more restrictive.*
- *(G177: CAT II) The SA will ensure the owner of global initialization files is root.*
- *(G179: CAT II) The SA will ensure the group owner of global initialization files is root, sys, bin, other, or the system default.*
- *(G181: CAT II) The SA will ensure global initialization files contain the command `mesg –n`.*
- *(G183: CAT II) The SA will ensure all default/skeleton dot files have permissions of 644, or more restrictive.*
- *(G185: CAT II) The SA will ensure the owner of all default/skeleton `dot` files is root or bin.*
- *(G187: CAT II) The user and SA will ensure global initialization files do not have a '.', or a '::' in the `PATH` variable definition except as the last entry.*

3.9.2 Local Initialization Files

Local initialization files (i.e., files in a user's home directory with a name that begins with '.') are files that are normally read by the kernel (or utility programs) and used to customize the user's environment. These files include `.login`, `.profile`, `.cshrc`, and other files that are used by a system's shell or other utilities to set the initial working environment whenever users log on or execute an application or system utility. A list of common UNIX home directory startup files is located in *Appendix B, Home Directory Security-Related Files*. Local initialization files will be owned by the user or root and will be no more permissive than 740. If a local initialization files, such as `.profile`, sets the `PATH` variable, it will not contain a '.' or '::' except in the last position. The `PATH` variable defines the search sequence the shell uses to find executable programs. A `PATH` variable may be observed by typing the `env` or `set` command, which will display a users environment configuration, or by typing `echo $PATH`, which will only display path data. The `PATH` is normally placed in the global initialization files (for global settings), or in each user's `.profile`, `.cshrc`, or `.login` file (depending on the user's shell). The `PATH` is constructed in the following format (for `sh` or `ksh`):

```
PATH=/bin:/usr/bin:/oracle/bin:/usr/local/bin
```

This indicates that when a user types a command name the shell will search `/bin` for the command first, and if the command is not found there, the shell will search for the command in `/usr/bin`, and so on. A. '.', '::' or, ':' as the last element of a `PATH` definition represents the current directory.

If a `PATH` variable is written as follows:

```
PATH=/bin:.:/usr/bin:/oracle/bin:/usr/local/bin
```

Then the shell would search the current directory for the command immediately after it searched `/bin`. Assume the user was in the `/tmp` directory (the current directory) when attempting to execute the `ls` command. Assume a malicious user created an executable program in `/tmp` named `ls`. Assume the `ls` program in `/tmp` executes a command to delete all of the user's files. If the user typed `ls` and the kernel did not find it in `/bin`, it would search the current directory, execute the malicious `ls`, and destroy all of the user's files. For this reason, it is preferable to never have a '.' in the `PATH` variable. Since it would be more disastrous if the above scenario happened to root, root will never have a '.' in the `PATH` variable.

Ensure user startup files are not executable by others and do not have the `suid` or `sgid` bits set, which could allow a malicious user to gain expanded privileges. To aid in the protection against introducing Trojan horses, the SA will ensure that system and user startup files do not execute world writable programs or scripts. Root's startup files are startup files in root's home directory that serve the same purpose for root as other user startup files do for users. Finally, startup files will not execute the `mesg –y` or `mesg y` command that would make their terminal devices world writable and open for possible exploitation.

- *(G199: CAT II) The SA will ensure the owner of users local initialization files is the user or root.*

- *(G201: CAT II) The SA will ensure local initialization files have permissions of 740, or more restrictive.*

- *(G203: CAT II) The user and SA will ensure local initialization files do not have a* **'.'**, *or a* **'::'** *in the* `PATH` *variable definition except as the last entry.*

- *(G205: CAT II) The SA will ensure local initialization files do not have the suid of sgid bit set.*

- *(G207: CAT II) The SA will ensure user local initialization files do not execute world writable programs.*

- *(G209: CAT III) The SA will ensure local initialization files do not contain the command* `mesg -y` *or* `mesg y`.

3.10 Trusted System/System Access Control Files

System access control (network) files establish parameters for UNIX systems to establish connections to and from other systems. The `.rhosts` and `hosts.equiv` files are used most often in establishing trust relationships between NIS/NIS+ hosts, but NIS/NIS+ is not necessary for setting up trust relationships. The **'+'** in the `/etc/passwd`, `/etc/shadow`, etc., files was used as a marker for systems to insert data from NIS maps. As this is no longer a requirement for the proper functionality of NIS and the **'+'** may allow unauthorized privileged access, the `/etc/passwd`, `/etc/shadow`, etc., files will not contain a **'+'**. The `.rhosts` (`.shosts` with SSH) and `hosts.equiv` (`shosts.equiv` with SSH) files can allow unrestricted system access with no I&A. The `.netrc` files are used to automate `ftp` sessions but they will not be allowed except where they are associated with the use of the `sftp`, or equivalent, command.

The `hosts.equiv` and `.rhosts` files are security files that authorize system access by remote hosts and by users on local or remote hosts. The `hosts.equiv` file and `.rhosts` files in users' directories specify remote hosts and users equivalent to the local host or user. Users from equivalent remote hosts are permitted to access local accounts using `rcp`, `remsh`, or `rlogin` without supplying a password. The `.rhosts` file is used to authorize users to access the specific account in which the `.rhosts` file is located (the `.rhosts` file is required to be owned by the user whose directory it resides in). The `hosts.equiv` file can authorize many users from a specific host. Refer to *Section 4.15, Secure Shell (SSH) and Equivalents*, for additional guidance on the use of `hosts.equiv`, `.rhosts` and `.shosts`.

- *(G211: CAT II) The SA will ensure* `.rhosts`, `.shosts`, `/etc/passwd`, `/etc/shadow`, `/etc/group`, *and* `hosts.equiv` *files will not contain a plus (+) unless defining entries for NIS+ netgroups.*

- *(G213: CAT II) The SA will ensure* `.netrc` *files do not exist.*

- *(G215: CAT II) The SA will ensure, if* `.rhosts`, `.shosts`, *and* `hosts.equiv` *files exist, will contain only lines with host-user pairs (e.g., host2 root) except in cases where they are defining netgroups for NIS+. These files will also to be justified and documented with the IAO.*

- *(G217: CAT I) The SA will ensure* `hosts.equiv`, `.rhosts` *nor* `.shosts` *are used, unless justified and documented with the IAO.*

- *(G219: CAT II) The SA will ensure, if* `.rhosts`, `.shosts`, *or* `hosts.equiv` *files exist, they will not be accessible by anyone other than the owner or root.*

- *(G221: CAT II) The IAO will not allow a trusted relationship with any system that is not also under the control of a security program that is acceptable to DOD.*

- *(G223: CAT II) The SA will ensure* `.rhosts` *is not supported in the pluggable authentication module* (*PAM).*

3.11 Shells

A shell is a program that serves as the basic interface between a user and the operating system. It is a command interpreter that accepts input from a user, interprets what is needed, and calls the appropriate kernel functions to accomplish requests. The shell also establishes the environment that a user operates in, or controls the user's view of the system. It may be modified to suit almost any user, and it may run additional programs that serve as additional layered front-end interfaces. Every system comes supplied with several shells (e.g., `sh`, `ksh`, `csh`, `bash`, etc.) that may be defined as the default shell for users. The IAO will ensure the validity of and approve these shells. The IAO will define the shells that users are allowed to use in a file called `/etc/shells`. This will prohibit the use of shells that have not been validated and approved for usage. Without this file, shells may be used with unknown results. If a user does not have a shell authorized through inclusion in this file, that user will not be able to log on. The SA may use shells not listed in the `/etc/shells` file to disable accounts. These are `/usr/bin/false`, `/bin/false`, `/sbin/nologin`, or `/dev/null`. They will not be included in the `/etc/shells` file because, though `ftp` uses a shell of its own, it first checks to see if the potential user has a valid shell by checking the `/etc/shells` file. If it finds the `/dev/null` shell definition there, for instance, and the login is not locked, it will allow an otherwise restricted user to log in with `ftp`.

- *(G225: CAT II) The SA will ensure the* `/etc/shells` *file exits.*

- *(G227: CAT II) The SA will ensure all shells referenced in the `/etc/passwd` file is listed in the `/etc/shells` file. The `/usr/bin/false`, `/bin/false`, `/dev/null`, `/sbin/nologin`, and `sdshell` will be considered valid shells for use in the `/etc/passwd` file, but will not be listed in the `/etc/shells` file.*

- *(G229: CAT I) The SA will ensure no shell has the suid bit set.*

- *(G231: CAT II) The SA will ensure no shell has the sgid bit set.*

- *(G233: CAT II) The SA will ensure the owner of all shells is root or bin.*

- *(G235: CAT II) The SA will ensure all shells have permissions of 755, or more restrictive.*

3.12 Device Files

A device file is a special UNIX file that is configured with major and minor device numbers. Major and minor device numbers identify the device special file and its characteristics to the UNIX kernel. They provide a linkage from the user to the UNIX device drivers that control peripheral and memory operations. Device drivers reside in the kernel. Device files reside in special directories. The device directory and device file access permissions, as well as device driver major and minor number integrity, are critical to system security. The function of a UNIX device file can be changed by changing the major and/or minor numbers associated with it. If the device directory, device special file, or a device driver is compromised, then the entire system could be compromised.

Device files located outside the normal locations may indicate attempts to compromise the system. For this reason, the system will be scanned weekly for extraneous device files. If extraneous device files are located, the IAO will investigate to identify the source and take appropriate action. Backup devices present a more subtle security hazard. If they are writable by any user except root or a pseudo backup user, a backup could be destroyed accidentally or maliciously or even altered. Files not usually accessible to users may be accessible from a world readable and writable backup device. Therefore, backup devices (normally devices controlling tape drives and system floppy disks) will not be world readable or writable.

Audio and video devices that are globally accessible have proven to be another security hazard. There is software that can activate system microphones and video devices connected to user workstations and/or X terminals. Once the microphone has been activated, it is possible to eavesdrop on otherwise private conversations without the victim being aware of it. This action effectively changes the user's microphone to a bugging device. Vendor procedures normally install `/dev/audio` (or the equivalent) with the device file permissions set to 666 (globally writable and therefore vulnerable). The SA and IAO will ensure the access permissions for the audio device are 644, or more restrictive. The audio device will be owned by root with a group owner of root, sys, or bin.

- *(G237: CAT III) All device files will be located in the directory trees as installed and designated by the operating system and/or application vendor.*

- *(G239: CAT III) The SA will ensure all local filesystems will be checked at least weekly against the system baseline to detect any extraneous device files.*

- *(G241: CAT II) The SA will ensure device file directories will not be writable except by the owner or as configured by the vendor.*

- *(G243: CAT II) The SA will ensure backup devices (tape and floppy disk device) and files will only be readable and writable by root.*

- *(G245: CAT II) The SA will ensure the audio devices have permissions of 644, or more restrictive.*

- *(G247: CAT II) The SA will ensure the owner of audio devices is root.*

- *(G249: CAT II) The SA will ensure the group owner of audio devices is root, sys, or bin.*

3.13 Special Purpose Access Modes

When the suid permission bit is set on an executable file, a user/process that runs the executable file is granted access based on the file's owner rather than the uid of the user/process that has executed the file. When the sgid permission bit is set on an executable file, similar to the suid permission bit, a user/process that runs the executable file is granted access based on the file's group owner rather than the gid of the user/process that has executed the file. Special operating characteristics may be assigned to a file or directory with the `chmod` command. These special characteristics are as follow:

set-user-id (suid)
set-group-id (sgid)
set sticky bit

3.13.1 Set User ID (suid)

Authorized, vendor-supplied suid programs are crucial to the correct operation of the UNIX operating system, but unauthorized suid programs present a security hazard. When the suid attribute is set on the access permissions of a program, a user executing the program has the same privileges as the owner of the program. If the owner of the program is root, then the user, while executing that program, has all the powers of root, at least for the scope of the program being executed. Therefore, it is extremely important that any program that has the suid bit set is of known origin and scope.

Refer to the specific vendor's UNIX documentation for details concerning suid programs. Commercial and Government-supplied applications may also contain programs with the suid bit set. If so, the vendor/proponent instructions must be followed.

If a mounted filesystem has any suid executable scripts or programs, a user who invokes the executable takes on the uid of the executable's owner. The owner of such suid executables is typically a privileged user, usually root. If a filesystem is exported, a remote user, who may be normal or privileged, may execute suid files and alter files mounted, but not exported, on the exporting host system. This is a serious vulnerability, which must be managed with the `mount` command options.

- *(G251: CAT II) The IAO will document the ownership, permissions, and location of any files having the suid bit set.*

- *(G253: CAT II) The SA will ensure all local filesystems will be checked at least weekly against the system baseline to detect any unauthorized suid files as well as unauthorized modification to authorized suid files.*

- *(G255: CAT II) The SA will ensure user filesystems, removable media, and remote filesystems will be mounted with the `nosuid` option.*

3.13.2 Set Group ID (sgid)

Authorized, vendor-supplied sgid programs are crucial to the correct operation of the UNIX operating system, but unauthorized sgid programs present a security hazard. The sgid bit only affects executable programs. When this attribute is set, the user executing the program has the same privileges as the group owner of the program. It is extremely important therefore, that any program that has the sgid bit set is of known origin and scope. Programs with the sgid bit set must never allow escapes to the command line.

Refer to the specific vendor's UNIX documentation for details concerning sgid. Commercial and Government-supplied applications may also supply programs with the sgid bit set. If so, then vendor/proponent instructions must be followed.

- *(G257: CAT II) The IAO will document the ownership, permissions, and location of any files having the sgid bit set.*

- *(G259: CAT II) The SA will ensure all local filesystems will be checked at least weekly against the system baseline to detect any unauthorized sgid files as well as unauthorized modification to authorized sgid files.*

3.13.3 Sticky Bit

If directories are other (a.k.a., world) writable, they can be accessed and changed by any friendly or malicious user with access to the system. In other words, the directories could be populated with erroneous, malicious, and harmful information, or even deletion of directory content from the system. In the event a directory is required to allow all users permission to write to this directory, such as the case of public directories (e.g., `/tmp`) the sticky bit must be set. This sticky bit protects the files within this directory by preventing a user from deleting other users' files also located in this public directory. When a sticky bit has been set on a directory, a file may only be deleted by the owner of the file, owner of the directory, or root. For that reason, world writable directories will only be allowed if they are public directories and have sticky bit set.

The sticky bit will not be used to justify the existence of world writable directories. The only authorized world writable directories are those temporary directories supplied with the system or those designed to be temporary file repositories. The setting is normally reserved for directories used by the system and by users for temporary file storage (e.g., `/tmp`) and for directories that require global read/write access. Since the public directory owner can change or delete any file within the public directory, all public directories will be owned by root or the COTS/GOTS default application user, and the sticky bit will be set. The group owner of all public directories will be root, bin, sys, or the COTS/GOTS default application group.

- *(G261: CAT II) The SA will ensure no world writable files exist and world writable directories are public directories.*

- *(G263: CAT III) The SA will ensure the sticky bit is set on all public directories.*

- *(G265: CAT II) The SA will ensure the owner of public directories is root or the application user.*

- *(G267: CAT II) The SA will ensure the group owner of public directories is root, sys, bin, or the application group.*

3.14 Umask

The umask is a kernel variable that controls the file access permissions assigned to newly created files and directories. Data and program integrity, confidentiality, and availability are directly affected by the system and user umask. Newly created files/directories will be accessible to unauthorized and possibly malicious users if the umask is too permissive. Additionally, applications may not function correctly if the umask is too restrictive. Therefore, the umask is a critical component of every user and system process.

The umask controls access permissions for the following three groups:

- File owner (or creator)
- Owner's default group
- Rest of the world (others)

By default, the system creates files with permissions of 666 and directories with permission to 777. To determine what permissions a given umask will assign to a newly created file, subtract the umask from 666. A 022 umask, for instance, would assign the file creator read and write permissions while assigning the group and world read permissions. The access permissions are read as 644. Most UNIX systems are fielded with a default umask of 022. This allows access permissions of 644 for files and 755 for directories. The umask must be configured to only allow access to the file by the owner of the file. To accomplish this, the system and user umask will be set to 077. Exceptions to this will be some applications, such as Oracle, which require an umask of 022, during software installation when the installation process demands a more permissive value, during database access by users, and during administrative actions. If required, only after explicit action by the owner (i.e., discretionary access control [DAC]) would file access be granted to group users and/or the rest of the world. All requirements will be justified and documented with the IAO.

- *(G269: CAT II) The SA will ensure the system and user umask is 077.*

- *(G271: CAT III) The SA will ensure applications requiring a umask are more permissive than 077, will be no more permissive than 022 and will be justified and documented with the IAO.*

3.15 Development Systems

Application developers often ignore security requirements in favor of development expediency. One of the most important parts of applications today, however, is security. Therefore, development systems will be subject to the same security requirements as production systems and are subject to SRRs by FSO. Development systems are often connected to live production networks and, because security requirements have not been observed, jeopardize the entire network. If network connectivity is a requirement for development systems, they will be connected to a testing network that is completely isolated from all other production systems and networks, such as with an isolated subnetwork. Applications will be designed to work correctly in a secure environment. Performing SRRs on development systems will help ensure secure practices are used in the development stages. This will avoid the problem of trying to retrofit security into newly released systems, hardware, and applications. If access to live test data is required, then a mirror of real data, that does not jeopardize personal data, will be used.

- *(G273: CAT II) The SA will ensure development systems are subject to the same security requirements as production systems.*

3.16 Default Accounts

UNIX systems come configured with default system accounts and, when software is installed, default accounts for applications. These accounts usually have default standard passwords. Default system accounts are normally listed at the beginning of the `/etc/passwd` file and have names like bin, lib, uucp, news, sys, guest, and daemon. They are usually disabled in the password or shadow file. The SA will also ensure system default accounts, other than root, are disabled by locking the password and the shell field will contain an invalid shell. The SA will ensure new passwords are assigned for applications, both internally (Oracle is shipped with a standard manager password of manager, for instance) and in the password and shadow files.

- *(G275: CAT I) The SA will immediately change any default passwords.*

- *(G277: CAT II) The SA will ensure logon capability to default system accounts (e.g., bin, lib, uucp, news, sys, guest, daemon, and any default account not normally logged onto) will be disabled by making the default shell `/bin/false`, `/usr/bin/false`, `/sbin/false`, `/sbin/nologin`, or `/dev/null`, and by locking the password.*

3.17 Audit Requirements

Auditing is not system logging and is not system accounting. System logging is done via the `syslog` facility. System accounting, when activated, collects data useful for charging timeshare customers and for system capacity planning.

C2 security requires monitoring of user and process activity almost to the keystroke level. It records much more detail about what users are doing and records system actions. Most systems provide system software for that purpose. Each is configured differently and has unique utilities for reading audit data files. Audit utilities can extract information about specific users and processes from the audit files. The IAO and SA will ensure audit files are only accessible to authorized personnel. Auditing will be configured to immediately alert personnel of any unusual or inappropriate activity with potential IA implications. The audit files will be retained for five years if the system contains sources and methods intelligence (SAMI); otherwise audit files will be retained for one year on backup media. All users, including root, will be audited. The SA will rotate and compress the audit logs one or more times a day to ease space requirements and to reduce the time required for log searches and reviews. Audit data will be backed up no less than weekly onto a different system or media than the system being audited. The implementation of an audit server will ease the attention required by audit logs and provide compliance with the requirement for the back up of audit data.

Red Hat Enterprise Linux 3 and SuSE Enterprise Server 8 has added an auditing subsystem, Linux Audit-Subsystem (LauS), that provides auditing of security-critical events and security functions that protect network-transmitted data. Earlier systems did not provide that auditing. SAs with earlier systems will obtain and implement third party software, such as `auditd` or `snare`, to ensure required auditing until the vendor supplies a workable auditing function or upgrades are applied. For earlier versions, and other vendors, third party auditing applications are available. All Linux platforms are subject to all auditing requirements.

- *(G279: CAT II) The SA will configure and implement auditing.*
- *(G281: CAT II) The SA will ensure audit data files and directories will be readable only by personnel authorized by the IAO.*
- *(G283: CAT I) The SA will ensure audit data files have permissions of 640, or more restrictive.*
- *(G258: CAT II) The SA will ensure all users are subject to identical audit parameters.*
- *(G287-G299: CAT II) The SA will configure the auditing system to audit the following events for all users and root:*
  - *Logon (unsuccessful and successful) and logout (successful)*
  - *Process and session initiation (unsuccessful and successful)*

- *Discretionary access control permission modification (unsuccessful and successful use of chown/chmod)*
- *Unauthorized access attempts to files (unsuccessful)*
- *Use of privileged commands (unsuccessful and successful)*
- *Use of print command (unsuccessful and successful)*
- *Export to media (successful)*
- *System startup and shutdown (unsuccessful and successful)*
- *Files and programs deleted by the user (successful and unsuccessful)*
- *All system administration actions*
- *All security personnel actions*

- *(G301: CAT II) The SA and/or IAO will ensure old audit logs are closed and new audit logs started daily.*
- *(G303: CAT II) The IAO will ensure the auditing software can record the following for each audit event:*
  - *Date and time of the event*
  - *Userid that initiated the event*
  - *Type of event*
  - *Success or failure of the event*
  - *For I&A events, the origin of the request (e.g., terminal ID)*
  - *For events that introduce an object into a user's address space, and for object deletion events, the name of the object, and in MLS systems, the object's security level*
- *(G305: CAT II) Auditing will be configured to immediately alert personnel of any unusual or inappropriate activity with potential IA implications.*
- *(G307: CAT III) The IAO will ensure audit files are retained at least one year; systems containing SAMI will be retained for five years.*
- *(G309: CAT III) The IAO will ensure audit files are backed up no less than weekly onto a different system or media than the system being audited.*

3.17.1 Audit Review Guidance

Collection of user and process audit information is only part of the process of system monitoring. Collected data will be examined and analyzed at least daily to detect any compromise or attempted compromise of system security. The basic commands to review the audit files on a Solaris system are `auditreduce` and `praudit`. The command to review audit files on a HP is `audisp`. The commands have ample options to allow viewing the information in many formats. Other systems use similar utilities for reviewing audit data. The IAO will review audit files daily to detect possible system compromise, malicious users, or users that may need more instruction.

- *(G311: CAT II) On a daily basis, the IAO will review the audit trails and/or system logs for the following:*
  - *Excessive logon attempt failures by single or multiple users*
  - *Logons at unusual/non-duty hours*
  - *Failed attempts to access restricted system or data files indicating a possible pattern of deliberate browsing*
  - *Unusual or unauthorized activity by System Administrators*
  - *Command-line activity by a user that should not have that capability*
  - *System failures or errors*
  - *Unusual or suspicious patterns of activity*

3.17.2 Audit Server

DISA FSO is implementing and fielding an Audit Server (AS). The AS will be fielded to DOD customers. It collects audit data from multiple hosts and stores it on writable CD-ROM. The system relieves disk space demands caused by audit data collection by storing the audit files on a centralized server at specified intervals. The AS is intended to augment the audit process. Audit requirements are not reduced or changed in any way due to the fact a site does not have an audit server.

- *(G313: CAT II) The IAO will ensure the audit server will be used if available.*

3.18 Cron

Cron is a job scheduling utility that controls jobs configured to run in the background on a recurring schedule. Cron determines the schedule and the jobs from configuration files called crontabs. Cron keeps track of each specific crontab creator and executes the programs with all the privileges of the crontab creator. Because of that, crontabs will not execute world or group writable programs nor will the programs be located in, or subordinate to, world writable directories.

3.18.1 Access Controls

Cron uses a file called cron.allow, populated by the SA, to determine which users are authorized to create crontabs. Cron uses a file called cron.deny, also populated by the SA, to deny access to specific users. If cron.allow is used, there is no absolute need to also have a cron.deny file, because users not listed in the cron.allow file will not have access by default. If there are no cron.allow or cron.deny files, the system assumes either everybody can access cron or nobody can access cron, depending on the system. Therefore, every system will have either a cron.allow file listing authorized cron users, or a cron.deny file, listing users not authorized to use the cron. Default system accounts (with the possible exception of root) will not be listed in the cron.allow file. If there is only a cron.deny file, the default system accounts (with the possible exception of root) will be listed there. In addition, access to the use of cron facilities will be authorized and documented with the IAO.

3.18.2 Access Permissions and Owners

The maximum access permissions for the cron.allow and cron.deny files will be 600. The cron.allow and cron.deny files will be owned by root with a group owner of root.

Cron has the capability to log its actions, and their success or failure, to a log file. The SA will ensure the system is configured to log all cron actions. The SA will also ensure the cron log access permissions are set to 600, or more restrictive. The owner for the cron log will be root. The group owner of the cron log file will be root, bin, or sys. The SA or IAO will review the cron logs on a daily basis to detect any possible problems.

Other files and directories associated with cron will be owned by root or bin with a group owner of root, sys, or bin. Crontabs will be owned by root or the crontab creator. Crontabs will have a maximum access permission of 600. The access permissions for the cron and crontab directories will be 755, or more restrictive.

3.18.3 Restrictions

A `crontab`, or any program executed by a `crontab`, will not relax the system umask unless the requirement has been justified and documented with the IAO.

Users will use the `crontab -e` command to create or edit all `crontabs` associated with their account name. This utility provides file locking to prevent multiple users from editing the same file at the same time and notifies the `cron` daemon when `crontabs` have changed so the `cron` daemon knows to reread the `crontabs`. It should also provide the correct access permissions to the `crontab`.

- *(G315: CAT II) The SA will control access to the `cron` utilities via the `cron.allow` and/or `cron.deny` file(s).*
- *(G317: CAT II) The SA will ensure the `cron.allow` file has permissions of 600, or more restrictive.*
- *(G319: CAT II) The SA will ensure `crontabs` do not execute group or world writable programs.*
- *(G321: CAT II) The SA will ensure `crontabs` do not execute programs located in, or subordinate to, world writable directories.*
- *(G323: CAT II) The SA will ensure the owner of `crontabs` is root or the `crontab` creator.*
- *(G325: CAT II) The SA will ensure default system accounts (with the possible exception of root) will not be listed in the `cron.allow` file. If there is only a `cron.deny` file, the default accounts (with the possible exception of root) will be listed there.*
- *(G327: CAT II) The SA will ensure `crontab`s have permissions of 600, or more restrictive, (700 for some Linux crontabs, which is detailed in the UNIX Checklist).*
- *(G329: CAT II) The SA will ensure `cron` and `crontab` directories have permissions of 755, or more restrictive.*
- *(G331: CAT II) The SA will ensure the owner of the `cron` and `crontab` directories is root or bin.*
- *(G333: CAT II) The SA will ensure the group owner of the `cron` and `crontab` directories is root, sys, or bin.*
- *(G335: CAT II) The SA is responsible for ensuring `cron` logging is implemented.*

- *(G337: CAT II) The SA will ensure `cron` logs have permissions of 600, or more restrictive.*
- *(G339: CAT II) The SA will ensure the `cron.deny` file has permissions of 600, or more restrictive.*
- *(G341: CAT III) The SA will ensure `cron` jobs will not execute a program that sets the umask to a value more permissive than 077, unless justified and documented with the IAO.*
- *(G343: CAT II) The SA will ensure the owner and group owner of the `cron.allow` file is root.*
- *(G345: CAT II) The SA will ensure the owner and group owner of the `cron.deny` file is root.*

3.19 At

The `at` utility reads commands from standard input and groups them together for deferred execution at a time specified by the user. Because `at` executes jobs with the privileges of the user, `at` will not execute world or group writable programs nor will the programs be located in, or subordinate to, world writable directories.

3.19.1 Access Controls

`At` uses a file called `at.allow`, populated by the SA, to determine which users are allowed to create `at` jobs. `At` uses a file called `at.deny`, also populated by the SA, to determine which users are specifically denied use of the `at` facilities. Users specifically allowed to use `at` are listed in the `at.allow` file. Users specifically denied access appear in the `at.deny` file. If neither `at.allow` or `at.deny` exist, then root is the only user allowed access to use `at`. However, if only an empty `at.deny` file exists, then anyone may use `at`. The `at.allow` file may exist without the `at.deny` file. The `at.deny` file may exist without the `at.allow` file, but will not be empty. Users not listed in the `at.allow` file, if it exists, will not be allowed access to `at.` Therefore, every system will have either an `at.allow` file listing authorized `at` users, or an `at.deny` file, listing users not authorized to use the `at`. Default system accounts (with the possible exception of root) will not be listed in the `at.allow` file. If there is only an `at.deny` file, the default system accounts (with the possible exception of root) will be listed there. In addition, access to the use of `at` facilities will be authorized and documented with the IAO.

3.19.2 Access Permissions and Owners

The maximum access permissions for the `at.allow` and `at.deny` files will be 600. The `at.allow` and `at.deny` files will be owned by root with a group owner of root.

Access permissions for the `at` (or equivalent) directory will be 755 or more restrictive. The owner and group owner of the `at` (or equivalent) directory will be root, sys, bin, or daemon.

3.19.3 Restrictions

At jobs, or any program executed by an at job, will not relax the system umask unless the requirement has been justified and documented with the IAO.

The IAO will ensure programs executed via the `at` utility are neither world nor group writable and that programs run by root are not writable by any except root, the user, or the application. In general, the user, root, or an application will own programs executed by `at`. The IAO will ensure programs executed using `at` are located in a directory where every directory in the path is owned by the user, root, or the application, and that none are world writable.

The IAO will maintain documentation of all recurring `at` jobs, who runs them, and why. `At` jobs should be converted to cron jobs if justified by recurring requirements. `At` jobs can contain commands to reschedule themselves. This feature should only be used if documented and justified with the IAO. Since `at` can run time-delayed jobs that may disappear after execution, `at` has the potential to be used by intruders or malicious users to gain unauthorized information or to obtain higher user privileges in absentia. Evidence may be hard to obtain. For that reason, `cron` logging will be enabled.

- *(G347: CAT II) The SA will ensure access to `at` will be controlled via the `at.allow` and/or the `at.deny` file(s).*

- *(G349: CAT II) The SA will ensure the `at.deny` file is not empty.*

- *(G351: CAT II) The SA will ensure default system accounts (with the possible exception of root) are not listed in the at`.allow` file. If there is only an `at.deny` file, the default accounts (with the possible exception of root) will be listed there.*

- *(G353: CAT II) The SA will ensure the `at.allow` and `at.deny` files have permissions of 600, or more restrictive.*

- *(G355: CAT II) The SA will ensure programs executed via `at` are not group or world writable.*

- *(G357: CAT II) The SA and `at` users will ensure `at` jobs do not execute programs in, or subordinate to, world writable directories.*

- *(G359: CAT II) The SA will ensure the* `at` *(or equivalent) directory has permissions of 755, or more restrictive.*

- *(G361: CAT II) The SA will ensure the owner and group owner of the* `at` *(or equivalent) directory is root, sys, bin, or daemon.*

- *(G363: CAT II) The SA will ensure* `at` *jobs will not execute a program that sets the umask to a value more permissive that 077 unless it is justified and documented with the IAO.*

- *(G365: CAT II) The SA will ensure the owner and group owner of the* `at.allow` *file is root.*

- *(G367: CAT II) The SA will ensure the owner and group owner of the* `at.deny` *file is root.*

3.20 Batch Access

`Batch` reads commands to be executed either immediately or later depending on CPU scheduling and priority. `Batch` is equivalent to the `at` command `at -q b -m now`, where `queue b` is a special `at` queue specifically for `batch` jobs.

`Batch`, unlike `at`, executes commands and requests serially. This avoids the high system load that could be caused by running several background jobs at once.

Since `batch` and `at` are related, and use the same allow, deny, and log files, the security constraints for `batch` will be the same as for `at`.

3.21 Kernel Tuning

This section provides discussion and requirements for kernel settings and parameters to greatly increase the security of a UNIX system.

3.21.1 Restrict/Disable Core Dumps

A core dump may provide valuable information for a programmer in the terms of debugging, but this is a rarely used debugging tool. In addition, core dumps may also contain sensitive data that is not intended for viewing by other users on the system. Core dumps will be disabled or the core dump data will be written to a directory expressly created for this purpose, owned and group owned by root, with permissions set to 700.

These requirements are further detailed in the *UNIX Checklist,* as these may or may not be applicable to all UNIX platforms and versions.

- *(G369: CAT III) The SA will ensure core dumps are disabled or restricted.*

- *(G371: CAT III) The SA will ensure the owner and group owner of the core dump data directory is root with permissions of 700, or more restrictive.*

3.21.2 Disable Executable Stack

Numerous security bugs, issues, and compromises are related to the default permission settings of executable stacks. To prevent many of these stack buffer overflow attacks, the executable stack will be disabled.

This requirement is further detailed in the *UNIX Checklist*, as this may or may not be applicable to all UNIX platforms and versions.

- *(G373: CAT II) The SA will ensure the executable stack is disabled.*

3.21.3 Restrict NFS Port Listening

The NFS server may be configured to ensure the NFS server only responds to NFS client requests that originate from a privileged port. A privileged port is a port less than 1024. This configuration provides security checking via the NFS server to enforce integrity on the part of the NFS clients. This integrity checking prevents system users from writing RPC-based applications that attempt to defeat the NFS client access control checking.

This requirement is further detailed in the *UNIX Checklist*, as this may or may not be applicable to all UNIX platforms and versions.

- *(G375: CAT II) The SA will ensure NFS client requests are restricted.*

3.21.4 Use Better TCP Sequence Numbers

To decrease the risk of session hijacking by an attacker predicting TCP sequence numbers, better TCP sequence numbers will be used.

This requirement is further detailed in the *UNIX Checklist*, as each UNIX platform may or may not provide this functionality or may or may not require this setting due to the default behavior of the particular UNIX platform.

- *(G377: CAT II) The SA will ensure better TCP sequence numbers are used.*

3.21.5 Network Security Settings

UNIX is a general-purpose operating system that provides for configuration of certain network parameters. These are low-level network parameters configured to provide enhanced security at the network level.

Ensuring the proper configuration of these network parameters can aid in the defense against a multitude of attacks such as ARP attacks, ICMP denial of service, SYN flood attacks, etc.

Some basic security network configurations, for example;

- Disable source routed packets.
- Disable, for Ipv6, source routed packets.
- Disable source routed return packets.
- Disable system directed broadcasts with IP forwarding is enabled.
- To increase the size of the unestablished connection queue.
- To increase the size of the established connection queue.
- Do not respond to ICMP timestamp requests.
- Do not respond to ICMP timestamp broadcast requests.
- Do not respond to echo request broadcasts.

This requirement is further detailed in the *UNIX Checklist*, as each UNIX platform provides similar security settings, with a different way to implement the security requirement. Each UNIX platform, as well as versions of a particular platform may implement the required network parameters in a different way.

- *(G379: CAT II) The SA will ensure network parameters are securely set.*

3.22 File Systems

The `/home`, `/export/home`, and `/var` filesystems will have their own partitions. If not properly partitioned, in the event that one of these partitions becomes full, the risk of the root partition becoming 100% full will occur, which may cause system and application issues.

- *(G381: CAT III) The SA will configure separate filesystem partitions for `/home`, `/export/home`, and `/var` unless justified and documented with the IAO.*

3.23 UFS

This is only for ufs filesystems. A corrupted root filesystem is one avenue an attacker with physical access to the system console can use to compromise the system. To reduce the likelihood of the event, enable the `logging` option. The SA may also want to enable the logging option to other ufs filesystems. This will help the system to reboot faster in the event of a crash. The cost in disk space is approximately 64MB per partition for the transaction log file.

The `largefiles` ufs mount option for filesystems will allow files larger than two gigabytes to be created. This is very useful for large databases and is the default for file mounts. The `nolargefiles` option may cause difficulties if the 2GB size limit is exceeded.

- *(G383: CAT II) The SA will ensure the `nolargefiles` option is not invoked unless justified and documented with the IAO.*

- *(G385: CAT II) The SA will ensure the* `logging` *option is implemented for the root filesystem.*

3.24 Syslog AUTH Facility

Security related data is sent via the AUTH facility, as such, the SA will ensure the authentication notice and informational data is configured to log to the AUTH facility.

- *(G387: CAT II) The SA will ensure the authentication notice and informational data is logged.*

This page is intentionally left blank.

4. NETWORK SERVICES

Most system services that can be accessed via the network are defined in the `inetd.conf` file. The `inetd.conf` file contains the configuration for the `inetd` program. The `inetd` program is a daemon that listens for network connection requests and services them by spawning another process. If the requested service is not defined in its configuration file, `inetd` will refuse to provide the service. Sites can limit the types of network services provided by commenting out the lines that define the service in the `inetd.conf` file.

This section is not intended to endorse the use of the services described. This is merely to familiarize the reader with the purpose of the service.

`Inetd` logging/tracing will be enabled. Tracing tells `inetd` to trace all incoming connections by logging the client's Internet address, TCP port number, and the name of the service using syslog.

The `inetd.conf` file will be owned by root or bin and have permissions of 440, or more restrictive. The `services` file will be owned by root or bin and have permissions of 644, or more restrictive.

The SA will be responsible for disabling network services not necessary for operations. These services will be disabled in the `inetd.conf` file and will not be allowed to run from inside, or outside `inetd`, or in any other fashion. Additionally, network services that are started by other means (e.g., run control scripts) must be disabled if not necessary for operations. Network services required for operations and are not disabled are to be documented with the IAO.

The Center of Internet Security (CIS) provides several UNIX/Linux benchmarks that contain industry standard security guidance, which may additionally aid the site in their UNIX/Linux security efforts. These benchmarks may be found at http://www.cisecurity.com.

- *(G389: CAT III) The SA will ensure all network services not required for operations are disabled. Any network services required for operations must be documented with the IAO.*

- *(G391: CAT II) The SA will ensure `inetd` is disabled (`xinetd` for Linux) if all `inetd` based services are disabled.*

- *(G393: CAT II) The SA will ensure the owner of the `inetd.conf` file is root or bin.*

- *(G395: CAT II) The SA will ensure the `inetd.conf` file has permissions of 440, or more restrictive.*

- *(G397: CAT II) The SA will ensure the owner of the `services` file is root or bin.*

- *(G399: CAT II) The SA will ensure the `services` file has permissions of 644, or more restrictive.*

- *(G401: CAT III) The SA will ensure `inetd` logging/tracing is enabled.*

4.1 Rlogin and rsh

The `rlogin` and `rlogind` programs provide remote terminal service similar to `telnet` and `telnetd`. The client program is `rlogin`, and the server program is `rlogind`. The important difference between `rlogin` and `telnet` is that if the `rlogin` connection is coming from a trusted host or a trusted user (i.e., `.rhosts` and/or `hosts.equiv` is properly configured), no password is required.

The `rsh` and `remsh` programs are similar to `rlogin`. The client program is `rsh`, and the server program is `rshd.` The `rsh` command requires no password if `.rhosts` and/or `hosts.equiv` is set up correctly.

Secure shell provides a functional and more secure alternative to the typical requirements for `rlogin` and `rsh`.

- *(G403: CAT I) The SA will ensure remote login and remote shell are not enabled.*

4.2 Rexec

The remote command execution daemon, `rexecd`, allows users to use `rsh` or `remsh` to execute commands on other systems. A password may or may not be required depending on the use of `.rhosts` and/or `hosts.equiv`. Unlike `login` and `telnet, rexecd` returns different error messages for invalid accounts and passwords. If an invalid username is supplied the error message returned is login incorrect. If an invalid password is supplied, it returns password incorrect. This allows a potential unauthorized user to probe the system to find a valid user account name and then to work on the password.

- *(G405: CAT III) The SA will ensure `rexec` is not enabled.*

4.3 Finger

The `finger` command makes personal information available to users on the network. Hackers use this feature to obtain and exploit information about users and to help obtain unauthorized access to accounts. The syntax is simple, `finger user@host`. The `finger` command output displays a user's information, such as login name, real name, terminal name, etc. The `finger` daemon will be disabled.

- *(G407: CAT III) The SA will ensure `finger` is not enabled.*

4.4 Remote Host Printing

The `/etc/hosts.lpd` (Berkeley Software Distribution [BSD]), `/etc/lp/Systems` (System V), `/etc/printer.conf`, or an equivalent file enables remote host printing on most systems. It is possible for unauthorized remote systems to print to hosts (as a print server) if the printer configuration files are not configured properly. All print clients and print servers will be documented with the IAO.

- *(G409: CAT II) The SA will ensure all print server and print client configurations are documented with the IAO.*

- *(G411: CAT II) The SA will ensure the local UNIX host printer configuration file, if one exists, does not contain the '-' (minus) or '+' character.*

- *(G413: CAT II) The SA will ensure the owner of printer configuration files is root, sys, bin, or lp.*

- *(G415: CAT II) The SA will ensure printer configuration files have permissions of 664, or more restrictive.*

4.5 Traceroute

`Traceroute` is a utility used to determine the path a packet takes between two points. If a packet filter firewall is configured incorrectly, an attacker can use the `traceroute` command, through the firewall, to obtain knowledge of the network topology inside the firewall. The information may allow an attacker to determine trusted routers and other network information that may lead to system and network compromise. `Traceroute` is often used by network management software.

- *(G417: CAT II) The SA will ensure the owner of the `traceroute` command is root.*

- *(G419: CAT II) The SA will ensure the group owner of the `traceroute` command is root, sys, or bin.*

- *(G421: CAT II) The SA will ensure the `traceroute` command has permissions of 700, or more restrictive.*

4.6 Client Browser Requirements

Navigator is a web browser client from Netscape Communications Corporation. Navigator has a number of security-related options that must be set. Netscape is no longer a vendor-supported product. Limited support is available for the Netscape Browser product through the DOD license agreement. Details about the DOD license agreement can be found at http://dii-sw.ncr.disa.mil/Del/netlic.html. More details concerning the support are available at http://netscape.intelligent.net/redisa/.

Commonly used open source web browsers include Mozilla, which is supported on Linux x86 and comes bundled with Solaris 9 and above. Firefox is also an open source web browser, which is supported on Linux i686.

The below requirements are for all browsers, these requirements ensure a more secure operating environment as well as protecting the UNIX system from authorized access and/or process (e.g., Active-X and Java Scripts).

- *(G423: CAT III) The SA will ensure the browser is capable of 128-bit encryption.*
- *(G425: CAT II) The SA will ensure the SmartUpdate, or software update feature, of a browser is not enabled.*
- *(G427: CAT II) The SA will configure browsers to disallow secure content caching unless encrypted.*
- *(G429: CAT III) The SA will configure browsers to disallow automatic downloading of active content.*
- *(G431: CAT III) The SA will configure browsers to disallow active scripting.*
- *(G433: CAT II) The SA will configure browsers to issue a warning if form data is redirected.*
- *(G435: CAT III) The SA will disable JavaScript on browsers.*
- *(G437: CAT II) The SA will configure browsers to issue a warning when viewing data on a remote site containing a security certificate that does not match its Internet address.*
- *(G439: CAT II) The SA will configure browser home pages for the local site home page or a blank page.*
- *(G441: CAT II) The SA will ensure browsers are configured for Secure Socket Layer (SSL) v2 and SSL v3.*

SSL v2 Enable	
X	RC4 encryption with 128-bit key
X	RC2 encryption with 128-bit key
X	Triple DES encryption with 168-bit key
X	DES encryption with 56-bit key
X	RC4 encryption with 128-bit key
X	RC2 encryption with 40-bit key

SSL v3 Enable	
X	RC4 encryption with 128-bit key and an MD5 MAC
X	Triple DES encryption with 168-bit key and a SHA-1 MAC
X	DES encryption with 56-bit key and a SHA-1 MAC
X	RC4 encryption with 40-bit key and an MD5 MAC
X	RC2 encryption with a 40-bit key and an MD5 MAC
	No encryption with an MD5 MAC

- *(G443: CAT I) The root account will not use a browser for any reason other than to control local applications.*

- *(G445: CAT II) The SA will ensure the browser is a supported version.*

- *(G447: CAT III) The SA will configure browsers to issue a warning when accepting/storing cookies.*

- *(G449: CAT III) The SA will configure browsers to issue a warning when entering an encrypted or secure site.*

- *(G451: CAT III) The SA will configure browsers to display a warning when submitting non-encrypted form data to an html page.*

- *(G453: CAT III) The SA will configure browsers to display a warning when viewing documents with both secure and non-secure content.*

- *(G455: CAT III) The SA will configure browsers to issue a warning when leaving an encrypted or secure site.*

- *(G457: CAT III) The SA will ensure Java is disabled on browsers.*

4.7 Sendmail or Equivalent

The Simple Mail Transfer Protocol (`smtp`) is the standard for transferring e-mail between hosts. The `sendmail` program or equivalent (e.g., `mmdf`, `rmail`, `smail`) implements both the client and server sides of the `smtp` protocol. `Sendmail` can deliver e-mail to local and remote users, mailing lists, and programs. E-mail addresses are located in an `aliases` file in which users, working through their electronic mail administrator, may establish e-mail addresses and mailing lists.

The `sendmail.cf` file contains the configuration parameters for the `sendmail` program. Two parameters, `expn` (expand) and `vrfy` (verify), are used somewhat like the `finger` command to provide e-mail information about users. The `expn` command can be used to expand a user's address to show the complete path to where the account is maintained. The `vrfy` command can be used to verify that a user has an account on the specific host. These commands are available, on an interactive basis, after connecting to a system on port 25. Because they deliver information that could be used to hack accounts, they will be disabled. `Sendmail` runs with root privileges and has had many security vulnerabilities associated with it, for those reasons, ensuring a secure configuration is of utmost importance. `Sendmail` has become a favorite object of hacker attacks. The SA will configure `sendmail`, or equivalent, to not display version information. This can be accomplished by changing the greeting line in `sendmail.cf` from:

```
O SmtpGreetingMessage=$j Sendmail $v/$Z; $b
```

to

```
O SmtpGreetingMessage= Mail Server Ready ; $b
```

If the system version of `sendmail`, or equivalent, supports the following features, they should also be entered into the `sendmail.conf` file:

`needmailhelo`
: Insists on the HELO/EHLO before accepting a MAIL command.

`restrictmailq`
: Restrict who can see the mail queue.

`restrictqrun`
: Restrict who can restart sending email in the mail queue.

- *(G459: CAT I) The SA will ensure `sendmail`, or its equivalent, will not allow the `kill` command.*
- *(G461: CAT II) The SA will ensure the `aliases` file is owned by root.*
- *(G463: CAT II) The SA will ensure the `aliases` file has permissions of 644, or more restrictive.*
- *(G465: CAT I) The SA will ensure programs executed through an `aliases` file entry are owned by root and reside in a directory that is owned by root.*
- *(G467: CAT II) The SA will ensure programs executed through an `aliases` file entry have permissions of 755, or more restrictive.*

- *(G469: CAT IV) The SA will ensure the `sendmail` logging level (the detail level of e-mail tracing and debugging information) in the `sendmail.cf` file is set to a value no lower than nine (9).*

- *(G471: CAT II) The SA will ensure critical-level `sendmail` messages are logged to a system log file.*

- *(G473: CAT II) The SA will ensure the owner of the critical `sendmail` log file is root.*

- *(G475: CAT II) The SA will ensure the critical `sendmail` log file has permissions of 644, or more restrictive.*

- *(G477: CAT III) The SA will ensure critical-level `sendmail` messages generate e-mail to the postmaster.*

- *(G479: CAT II) The SA will ensure the e-mail software does display addresses through the `rcpt` command.*

- *(G481: CAT II) To help mask the e-mail version, the SA will use the following in place of the original sendmail greeting message:*

```
O SmtpGreetingMessage= Mail Server Ready ; $b
```

- *(G483: CAT I) The SA will ensure `.forward` files are not used.*

- *(G485: CAT I) The SA will ensure all `sendmail` security patches are incorporated or the latest vendor version of `sendmail` is loaded.*

- *(G487: CAT I) The SA will ensure `sendmail`, or its equivalent, will not allow the `debug` command.*

- *(G489: CAT I) The SA will ensure the `decode` entry is disabled (deleted or commented out) from the alias file.*

- *(G491: CAT III) The SA will ensure the `expn sendmail` command is disabled.*

- *(G493: CAT II) The SA will ensure the `vrfy sendmail` command is disabled.*

- *(G495: CAT I) The SA will ensure `sendmail`, or its equivalent, will not allow the `wiz` or `wizard` commands.*

4.8 FTP and Telnet

Under certain circumstances the use of FTP and telnet may be the only viable solution (primarily due to legacy applications); however, the use of FTP and telnet is not a recommended best practice. The use of clear text transmission will be phased out as quickly as possible and the use of encrypted sessions will be implemented in the architecture. The use of an encrypted session is required if supported by the device.

If encryption protocols such as SSL or SSH transmit traffic directly to a host, then a host based intrusion detection (HID) system must be employed on the device if supported. All network traffic must be visible to an Intrusion Detection System (IDS). VPN traffic will not bypass the security architecture and must terminate in order for the traffic to be processed by a network intrusion detection (NID) system.

FTP and telnet are permissible inside an enclave, behind the premise router and protected by a firewall and router access control lists (ACLs); however, the requirement must be justified and documented with the IAO. If either of these services is not required, the service will be deleted, disabled or turned off. If the service is disabled, the site will continue to ensure that all appropriate patches are applied. When used, all associated traffic will be restricted by IP source and destination address if technically feasible. Under no circumstances will FTP or telnet be used with a uid and password that has administrative or root privileges.

- *(G497: CAT II) The SA will ensure FTP and telnet within an enclave is behind the premise router and protected by a firewall and router access control lists.*

- *(G499: CAT II) The SA will ensure FTP and telnet within an enclave is justified and documented with the IAO.*

- *(G501: CAT I) The SA will ensure FTP and telnet from outside the enclave into the enclave is not permitted, unless encrypted and the following conditions apply:*

    - *FTP and telnet are acceptable from outside the enclave through a remote access Virtual Private Network (VPN). The connection will terminate outside the firewall as to not bypass the security architecture. The connection will be proxied at the firewall or via an FTP/telnet proxy.*

    - *FTP and telnet are acceptable via a site-to-site VPN between trusted enclaves; however, the risk will be accepted as part of the accreditation package, System Security Authorization Agreement (SSAA) or an Acceptance of Risk letter (AORL) must already be in place for the tunnel. FTP and telnet are acceptable within distributed enclaves, if required, as long as the traffic is physically or logically segregated from normal traffic using a method supported by the network technology to create a virtual connection (e.g., VLAN, VPN, LANE, MPLS, IPSec tunnels).*

Under no circumstances will FTP or telnet be used with a userid (UID)/password that has administrative or root privileges.

- *(G503: CAT I) The SA will ensure userids/passwords used for FTP and telnet do not have administrative or root privileges.*

System-to-System FTP accounts (no user intervention) may be treated as an Application-type account and the password will be changed at least once a year or when an administrator with knowledge of the password leaves. When FTP is used for system-to-system FTP, an AORL is required. A system-to-system transfer via a VPN would not require an AORL.

The AORL will be used to document the use of unencrypted FTP or telnet or the risk will be accepted as part of the accreditation package, SSAA. The customer (data owner), the local DAA (when the site is not the data owner) will sign an acknowledgement of risk letter. The IAO will maintain the AORL. This AORL will identify the UIDs, passwords, and the data that is being transmitted unencrypted inside the site's enclave. The AORL will be dated and will be reviewed and renewed at least every 18 months.

- *(G505: CAT II) The IAO will ensure an AORL is used to document the use of unencrypted FTP and telnet or the risk will be accepted as part of the accreditation package.*

An anonymous FTP connection within the enclave will not be allowed. Individual uids will be created for each user. This requirement should not be confused with an anonymous FTP server. An anonymous FTP server is a special purpose server, which is used to distribute information (files, educational material, etc.). An anonymous FTP server utilizes an unauthenticated default username such anonymous or ftp and a commonplace password such a guest. An anonymous FTP server is permitted as long as (1) the server is compliant with the applicable *Operating System STIG*; is segregated into the network Demilitarized Zone (DMZ); is on its own subnet on a dedicated system; and as long as it only houses public information (information approved by the Public Affairs Officer, or equivalent).

- *(G507: CAT II) The SA will ensure anonymous* `ftp` *is documented with the IAO.*

- *(G509: CAT II) The SA will ensure anonymous* `ftp` *is segregated into the network DMZ.*

- *(G511: CAT II) The SA and IAO will ensure an anonymous* `ftp` *server houses only public information.*

4.8.1 FTP Configuration

When FTP is used to contact a remote host, the remote host requires the use of a valid account and password. FTP logons are recorded in the `/var/adm/wtmp` file. The `ftpusers` file allows identification of who may not use FTP to transfer files. This file is required for the vendor-supplied version and for encrypted versions of `ftp` and/or `ftpd`. At a minimum, it will contain all the default system users and root, have access permissions of 640, or more restrictive, and be owned by root with a group owner of root or bin. The FTP daemon will be owned by bin or root and have access permissions no more permissive than 755. `Ftpd` will be configured in the `inetd.conf` file and, on systems that support the logging and/or verbose options; `ftpd` will be configured with the `-l` and/or `-v` options to increase the level of logging.

- *(G513: CAT II) The SA will ensure the `ftpusers` file exists.*
- *(G515: CAT II) The SA will ensure the `ftpusers` file contains the usernames of users not allowed to use ftp, and contains, at a minimum, the system pseudo-users usernames and root.*
- *(G517: CAT II) The SA will ensure the owner of the `ftpusers` file is root.*
- *(G519: CAT II) The SA will ensure the `ftpusers` file has permissions of 640, or more restrictive.*
- *(G521: CAT II) The SA will ensure the owner of the `ftp` daemon is root or bin.*
- *(G523: CAT III) The SA will ensure systems using `ftpd` are configured with the logging (-l) and/or verbose (-v) options.*
- *(G525: CAT I) The SA will implement the anonymous `ftp` account with a non-functional shell such as `/bin/false`.*
- *(G527: CAT I) The SA will implement anonymous `ftp` using all system security recommendations.*
- *(G529: CAT II) The SA will ensure the ftp users `umask` is 077.*

4.9 File Service Protocol (fsp)

`Fsp` is an alternative to `ftp` that transfers files using User Datagram Protocol (UDP) rather than TCP. The majority of `fsp` activity is illegitimate. Any server running `fsp` should be thoroughly investigated for possible software piracy or intrusion.

- *(G531: CAT I) The SA will ensure `fsp` is not enabled.*

4.10 Trivial File Transfer Protocol (tftp)

`Tftp` is a file transfer program that requires no I&A. Normally, commenting it out of the inetd.conf file will disable it. `Tftp`, if required by a site, will be justified and documented with the IAO. The `tftp` daemon will be run in secure mode when that option is available. For instance, Solaris systems allow the `-s` option as an argument when invoking the `tftp` daemon. The SA will also ensure specific pathnames are defined to limit the paths available to the `tftp` daemon for reading and writing. Some `tftp` implementations incorrectly assume that `tftpd` should have the suid bit set to overcome directory access permissions. If the SA configures `tftp` correctly, however, this problem can be easily overcome. Therefore, setting the suid or sgid bits on the `tftp` daemon will not be allowed.

- *(G533: CAT I) The SA will ensure the secure mode option is used if `tftp` is implemented on a system that supports it.*

- *(G535: CAT I) The SA will ensure `tftpd` does not have the suid or sgid bit set.*

- *(G537: CAT II) The SA will ensure implementations of `tftp` will be configured to vendor specifications and will include the following:*

  - *A `tftp` user will be created.*
  - *The default shell will be set to `/bin/false`.*
  - *A home directory owned by `tftp` will be created.*

- *(G539: CAT I) The SA will ensure all `tftp` implementations are justified and documented with the IAO.*

4.11 X Windows

Used mainly in UNIX, X Windows is a windowing system that allows for the display of graphics via the network. This network-based display provides users with a GUI based console without having to be physically located at the UNIX server. The `xhost` and `xauth` commands are two basic X Windows commands for security. They each authorize X Windows users to the server. The `xhost` command authorizes hosts by name. The `xauth` command authorizes X Windows connections using an encoded string to identify host and client. The `xhost +` command, without arguments, authorizes all hosts to access X Windows. The `xhost -` command, without arguments, removes access rights from all hosts that are not on the access list. The command `xhost +hostX` would add a host called hostX to the access list. The command `xhost -hostX` would remove it from the access list. The `xhost` command creates a file called `X0.hosts` to list authorized hosts in (the access list).

The `xauth` command (in conjunction with some other X Windows commands) writes a file called `.Xauthority` in the home directory of each user who invokes X Windows. The `.Xauthority` file helps ensure the X Terminal user is the only one who can run programs on their X Terminal. The `xauth` program can also be invoked to edit the `.Xauthority` file to expand or restrict access privileges to the X Client. The `.Xauthority` file contains security information passed between the X Client and the X Server to authorize access to the X Server by the X Client. The information allows the X Client to open windows from the X Server. The file will be protected, therefore, with an access permission of 600, or more restrictive. The `xhost` command overrides the `.Xauthority` file and should not be used unless it is followed by the `xhost -` command when finished. The local X Server stores files in `/tmp/.X11-unix`. Ensure no other process can delete the `X0` file, and set the sticky bit on the `/tmp/.X11-unix` (and all .X11 subdirectories in `/tmp`).

- *(G541: CAT II) The SA will ensure each X Windows host will be configured to write .Xauthority files, or the equivalent, into each X Windows user's home directory.*

- *(G543: CAT II) The SA will ensure .Xauthority files have permissions of 600, or more restrictive.*

- *(G545: CAT I) The `xhost +` command will not be used to globally authorize X Clients.*

- *(G547: CAT II) X Clients that are authorized to connect to X Server display will be listed in the `X*.hosts`, or equivalent file(s) if the `.Xauthority` utility is not used.*

- *(G549: CAT II) The SA will ensure remote X-terminal access host is limited to authorized X clients.*

4.12 UNIX to UNIX Copy Program (uucp)

The `uucp` utility is designed to assist in transferring files, executing remote commands, and sending electronic mail between UNIX systems over phone lines and direct connections between systems. The u`ucp` utility is a primitive and arcane system with many security issues. There are alternate data transfer utilities/products that can be configured to more securely transfer data by providing for authentication as well as encryption. The `uucp` (and `nuucp`) utility will be disabled.

- *(G551: CAT II) The SA will ensure `uucp` and `nuucp` are not enabled.*

4.13 Simple Network Management Protocol (snmp)

The *Network Infrastructure STIG* should be referred to for specific and authoritative snmp information. This *STIG* provides secure set-up of some snmp configuration files on UNIX systems. Most vendors ship systems with snmp configured to start at boot-up and to honor snmp requests from any host or program that knows the default passwords. The default passwords are the same for all a vendor's systems, so it represents a significant security risk if allowed to run indiscriminately. Whether snmp is required or not, ensure the default snmp access passwords are changed to unique values.

Snmp servers will be configured to only run snmp software, network management software and such data base management systems as the network management system requires. Snmp will be disabled if not required.

Improperly configured snmp is a great tool for malicious users and intruders to obtain system and network information and for crashing systems and networks. An intruder or malicious user can learn system and network architectures, change system and network configurations, and shut down systems and networks by using carefully constructed snmp queries and messages. Ensure snmp configuration files (i.e., Management Information Bases (MIBs)) are owned by root and have a group owner of sys or the application. Also, ensure the snmpd.conf file is owned by root with a group owner of sys.

Although some snmp systems include provisions for password-based security, others do not. Version 2.0 of snmp was intended to include better security features, but it has not been made a standard.

Ensure the community string in the snmpd.conf file is changed from the default (public) to some other value determined by following the password controls defined for application passwords. By changing the community string from public to an acceptable password, the amount of information that a potential attacker can learn using snmp is limited. Ensure the MIB is not world writable or readable and is owned by root. When an snmp monitoring program (management station) queries an snmp client for information, the monitoring program must provide the correct community string or the client does not return any information.

- *(G553: CAT I) The SA will ensure snmp passwords are changed from the default and will not be guessable.*

- *(G555: CAT II) The SA will ensure the snmpd.conf file has permissions of 700, or more restrictive.*

- *(G557: CAT II) The SA and network administrator will ensure MIB files have permissions of 640, or more restrictive.*

- *(G559: CAT II) The SA will ensure the owner of the snmpd.conf file is root with a group owner of sys and the owner of MIB files is root with a group owner of sys or the application.*

- *(G561: CAT II) The IAO will ensure* `snmp` *servers only run* `snmp` *server software, network management software and such data base management systems as the network management system requires.*

4.14 System Logging Daemon (syslogd)

The system-logging daemon, `syslogd`, reads and forwards system messages to the log files and/or users. Malicious users can flood the logging daemon with unauthorized messages unless `syslogd` is configured to accept messages only from designated hosts. System logging normally takes place over port 514. Services to this port should be restricted to local hosts at the firewall or premise router.

If `syslogd` is required to log system messages to the local machine, ensure the system name in `/etc/hosts` contains the alias `loghost`. If the `/etc/hosts` file shows the loghost as some other system, then system log messages will be sent to that host instead of being logged on the local host. The IAO will maintain documentation of the machines using a non-local loghost. Local hosts will not be permitted to act as loghosts for systems outside the local network. Some messages need to be reviewed immediately by responsible parties such as root. Use the following example (or one similar) in the `/etc/syslog.conf` file to ensure alerts are written to the terminal screen of root or operator if they are logged on:

```
*.alert root,operator
```

- *(G563: CAT II) The SA will ensure the owner of the* `/etc/syslog.conf` *file is root with permissions of 640, or more restrictive.*

- *(G565: CAT II) The SA will ensure the group owner of the* `/etc/syslog.conf` *file is root, sys, or bin.*

- *(G567: CAT II) The SA will ensure local hosts are not configured to act as loghosts for systems outside the local network.*

- *(G569: CAT II) The SA will ensure machines using a non-local loghost will be documented with the IAO.*

4.15 Secure Shell (SSH) and Equivalents

SSH is a communications software that uses encrypted communications to log on to and perform tasks on other computers. It can also be used to execute remote commands and to transfer files between systems using the `sftp` sub-process. SSH communicates using encryption to protect data and passwords. It provides strong authentication and secure communications over insecure channels. SSH also provides `rlogin`, `rsh`, `rcp`, and `rdist` services, but since the communications are encrypted, it is done in a much more secure manner than traditional services. The use of SSH Tectia, OpenSSH, F-Secure, Reflection for Secure IT, or similar programs are some methods for accomplishing this.

Hackers, curious administrators, employers, and criminals, both industrial and government can eavesdrop on network communications using sniffers to collect private and corporate information such as account names, passwords, and sensitive data. Communication packets also include information about destination and origination network addresses. A sniffer is a program that puts a network interface into promiscuous mode. The interface, when in promiscuous mode, listens to all communication packets passing through the network instead of just packets that contain its destination address.

It is also possible to hijack unencrypted network connections. This technique can be used to enter in the middle of existing connections to modify data in both directions and to insert new commands in sessions authenticated by one-time passwords.

SSH connects to the Secure Shell daemon (`sshd`) on the server machine. It verifies the server machine really is the intended server machine. SSH then exchanges encryption keys (protected from sniffers), and performs authentication, RSA (Rivest, Shamir, and Adleman) authentication or conventional password based authentication. The server normally allocates a pseudo-terminal and starts an interactive shell or user program. SSH will also work with X Windows and provides encrypted replacements for `rlogin, rsh, rcp, rdist,` and `ftp`, as well as for `telnet`.

Several versions of Secure Shell are in use. FSO recommends the latest vendor version of the particular version of Secure Shell, or equivalent, used by the site. As of this writing, the current version of OpenSSH is SSH-2.0-OpenSSH_4.0p1. For SSH Tectia client/server solution version (previously SSH Secure Shell for Workstations or previously SSH Secure Shell for Servers, respectively) is 4.2. For Reflection for Secure IT (formerly F-Secure SSH) is 6.0.

There are two protocol versions (1 and 2) for all known versions of SSH. Due to the security concerns and integer overflow vulnerabilities with protocol version 1, protocol version 1 will not be used.

SSH may need to be compiled, depending on the source. In most cases, installation is simple, but OpenSSH requires the user to obtain and install a couple of other UNIX libraries. Some versions of OpenSSH have a problem working correctly with the Basic Security Module (BSM) on Solaris because of a lack of interaction with the pluggable authentication module (pam). This can be solved by compiling it with the following options: `'--with-pam'` or `'--with-tcp-wrappers'`, in order to get it to work with TCP_WRAPPERS.

SSH offers the ability to log on directly as root even when the system configuration files disables that feature for other access methods. Ensure this feature is disabled. SSH also allows the use of `.rhosts` or `.shosts`. These features are not to be used unless the feature is operationally necessary and is documented with the IAO. Refer to *Section 3.10, Trusted System/System Access Control Files*, for guidance on the use of .rhosts. It should be disabled in the `sshd_conf` file. Refer to *Section 3.3.1, Encrypted Root Access*, for security requirements for root when using SSH.

SSH can be used with X-windows by enabling port forwarding. This is enabled by default in the configuration file that comes with the source package.

- *(G571: CAT I) The IAO and SA will ensure SSH Protocol version 1 is not used, nor will Protocol version 1 compatibility mode be used.*

- *(G573: CAT I) The SA and IAO will ensure SSH, or a functionally similar utility, is used to encrypt all communications by all personnel, except from the system console to the system console device. The sole exception is for systems in the demilitarized zone (DMZ).*

- *(G575: CAT II) The SA will ensure SSH is configured to work with TCP_WRAPPERS except in cases where the encryption utility can be configured for IP filtering and still display banners before granting access.*

4.16 UNIX Routing Vulnerabilities

The *Network Infrastructure STIG* should be referred to for specific and authoritative reference material for routing. This *STIG* provides secure set-up of some routing configuration files on UNIX systems.

Routing bears no relationship to Domain Name System (DNS), although it does depend on the operation occurring before routing can take place. Routing is the process of reading the destination IP address in the header of a TCP or UDP packet and selecting the best route to send the packet to its destination. Routes are gained by a router from direct data entry, dynamically, or from other routers using Routing Information Protocol (RIP), RIP-2, Open Shortest Path First (OSPF), and other protocols. UNIX systems can be configured as routers.

Some vendors (e.g., Sun) ship systems that will automatically configure routing unless the administrator first configures a default gateway. A default gateway is a router the UNIX host will use for routing packets to their destination. Ensure route discovery is disabled by configuring a default gateway. If the machine is not used for routing, ensure IP forwarding is disabled. The file `/etc/norouter` (a Solaris only configuration file used to disable IP forwarding prior to Solaris 9) will be owned by root with a group owner of sys and permissions of 400.

Some vendors ship systems with the RIP software. RIP is older and more easily spoofed (allowing intruders to change the routing table information) than newer protocols such as RIP-2 or OSPF.

One way to determine if a system is currently running a routing protocol is to execute the `netstat –r` command. The output should be similar to the following:

ROUTING TABLE					
Destination	***Gateway***	***Flags***	***Reference***	***Use***	***Interface***
192.136.137.192	Nonstigunix	U	3	6	hme0
224.0.0.0	Nonstigunix	U	3	0	hme0
default	192.136.137.193	UG	0	2	
localhost	Localhost	UH	0	8	lo0

The reference to `default` (the third item in the Destination column, meaning default gateway) means the machine obtains its routing information from the default gateway and does not need to run the `route` daemon (e.g., `routed`, `in.routed`, or `gated`). If there is no default gateway defined, then the command will show many more routes (addresses) or a routing table, and the following commands will show that routing is enabled:

```
ps –ef | grep rout    (For Solaris)
ps –ef | grep gated   (For HP)
```

If this is the case, the IAO and the IAM will maintain documentation indicating the machine is being used as a router and indicate which systems it exchanges routing information with directly.

- *(G577: CAT II) The SA will ensure systems not running routing have a default gateway defined.*

- *(G579: CAT II) The IAO will ensure routing is implemented only on dedicated hardware. Systems used as routers will be documented with the IAO.*

- *(G581: CAT II) The SA will ensure the owner of the `/etc/norouter` file is root with a group owner of sys and permissions of 400.*

4.17 Lotus Domino Web Application

Lotus Domino is a Web application and messaging server. Lotus Domino Server version 5.0.5 could allow a remote attacker to traverse directories on the Web server. A remote attacker can request a URL containing `.nsf`, `.box`, or `.ns4` with dot dot sequences (`/../`) to read sensitive files on the Web server. In order to exploit this vulnerability, the server must be installed under the root directory.

- *(G583: CAT III) The SA will ensure the Lotus Domino Web Application is not vulnerable to the `.nsf`, `.box`, and `.ns4` directory traversal exploit.*

4.18 Squid Web Proxy

Squid is a freely available Web Proxy software package included with some Linux distributions.

4.18.1 Authentication Header

Squid Web Proxy Cache versions 2.x up to and including 2.4.STABLE6 could disclose sensitive information. Under certain conditions, the Squid proxy authentication header could be forwarded to external web sites, which could allow a remote attacker to obtain the proxy username and password.

- *(G585: CAT III) The SA will ensure the Squid Proxy Cache server is not vulnerable to the authentication header forwarding exploit.*

4.18.2 MSNT Auth Helper

Squid Web Proxy Cache versions 2.x up to and including 2.4.STABLE6 are vulnerable to a buffer overflow in the MSNT auth helper component. Under certain configurations, a remote attacker could overflow a buffer and execute arbitrary code on the system or cause the proxy server to crash.

- *(G587: CAT II) The SA will ensure the Squid Proxy Cache server is not vulnerable to the MSNT auth helper buffer overflow exploit.*

4.18.3 Version

Squid Web Proxy Cache is running on the system. A rogue proxy server could intercept, redirect, or reject valid web requests. The version must be 2.7STABLE7 or later.

- *(G589: CAT III) The SA will ensure the Squid Proxy Cache server is not a vulnerable version.*

4.19 iPlanet Web Server

iPlanet Web Server (now known as The Sun Java System Web Server) versions 4.1 and 6.0 could allow a remote attacker to view any file on the server, caused by a vulnerability in iPlanets search engine. A remote attacker could send a search command containing the path to a known file specified using dot dot sequences (e.g.,) as a value for the `NS-query-pat` parameter, which would cause the search engine to return the contents of the requested file.

- *(G591: CAT III) The SA will ensure the iPlanet Web Server is not vulnerable to the search engine NS-query-pat file viewing vulnerability.*

4.20 Network Filesytem (NFS)

Network Filesystem (NFS) allows clients to access filesystems located on remote servers as though the filesystems were resident on the clients. This allows a filesystem to be stored in one common location and securely exported to many clients at once instead of replicating it across many systems. NFS has the capability to enforce security policies for exported/shared filesystems. A security concern is presented with NFS because filesystems are physically located on remote servers and users can access and change the data without logging on to the server. This would appear to defeat the I&A requirements. This is also true for remote databases. If access to files is properly restricted, however, file security can be greatly enhanced.

Several steps are required to secure NFS against most forms of unauthorized access. The file (either `/etc/exports` or `/etc/dfs/dfstab`) contains a list of directories that are being exported and any restrictions, attributes, or options associated with them. This export file will be protected against unauthorized modification. Exported/shared system files will be owned by root and will not be world or group writable. Filesystems exported as other than read only will be documented with the IAO. These steps prevent sensitive system files from being modified or replaced.

Several options must be enabled in the NFS server file export configuration file. The NFS server must be configured to disallow access from client requests that do not include a userid. Access to exported filesystems must be restricted to local hosts via the export configuration file. The default userid mapping of root to exported filesystems will not be modified, and will not be used unless authorized and documented with the IAO. Solaris additionally provides a `secure` option that is used if Secure RPC (true if NIS+ is enabled on the system) is enabled on the system, NIS or NIS+ also is required for proper functionality. NIS or NIS+ is used to house and distribute public and encrypted secret. This allows NFS to use DES (Data Encryption Standard) for encrypting the authentication session between the server and client. Solaris systems must not set the sec option to none, the current default for the sec option allows for system authentication. In turn, the default is not be modified.

NFS clients will use the `nosuid` and `nosgid` options to mount filesystems from a server to prevent setuid and setguid executables of dubious origin from gaining root access on the client system.

Port monitoring causes NFS requests that do not come from privileged ports to be rejected. Port monitoring will be enabled.

Because NFS presents such a target of opportunity for attackers, the NFS daemons will not be allowed to run unless NFS is actually being used.

- *(G593: CAT II) The SA will ensure, if NFS is running, NFS port monitoring will be enabled.*
- *(G595: CAT II) The SA will ensure the owner of the export configuration file file is root.*
- *(G597: CAT III) The SA will ensure the export configuration file has permissions of 644, or more restrictive.*
- *(G599: CAT II) The SA will ensure filesystems are exported as read only unless an operational requirement warrants otherwise and has been justified and documented with the IAO.*
- *(G601: CAT II) The SA will ensure the owner of exported system files and directories is root.*
- *(G603: CAT II) The SA will ensure the NFS server is configured to disallow access from client requests that do not include a userid.*
- *(G605: CAT II) The SA will ensure access to exported filesystems is restricted to local hosts via the export configuration file.*
- *(G607: CAT II) The SA will ensure the* `sec` *option is not set to* `none`*; additionally the default authentication is not to be set to* `none`*.*
- *(G609: CAT II) The SA will ensure root access options are not used unless justified and documented with the IAO.*
- *(G611: CAT II) The SA will ensure NFS clients will mount filesystems with the* `nosuid` *and* `nosgid` *options set.*

4.21 Domain Name System (DNS)

The *DNS STIG* contains the latest reference material for DNS. The *DNS STIG* should be referred to for specific and authoritative DNS information. This *STIG* entry is meant only as a general guide for the use of DNS in the UNIX operating system arena. As this *UNIX STIG* does not encompass all security requirements for the secure operation of DNS, the *DNS STIG* will be used to ensure all DNS security requirements are complied with. DNS is an Internet service that translates domain names into IP addresses as well as translating IP addresses to domain names. Domain names, such as machine.disa.mil, are alphabetic because they are easier to remember. The Internet, however, is based on IP addresses. Every time a domain name is used, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name machine.disa.mil might translate to IP address 198.105.232.4. The Berkeley Internet Name Domain (BIND) is one of the implementations of DNS that was designed for Berkeley UNIX operating systems such as BSD, but has been adapted to most other vendor systems.

BIND, `named` and `in.named` are the same DNS software (without the configuration files). Systems other than the common HP and Sun systems may refer to the software by a different name. The `named` (or `in.named`) daemon is the software that implements BIND. The name/address resolver library included in the BIND distribution provides the standard application program interfaces (APIs) for translation between domain names and IP addresses. The resolver library is used for linking with applications requiring DNS. BIND has been plagued with security problems in all known versions. At this writing, version 9.3.1, 9.2.5, and 8.4.6 is the latest, and most reliable, distribution of the Internet Software Consortium (ISC) version of BIND.

Configuration files associated with BIND are as follows:

`/etc/resolv.conf`	Contains the domain and the server to use for address lookups
`/etc/named.conf`	Configuration boot file (contains locations of other files/tables)

The DNS translation tables defined in `named.conf`

`/var/run/named.pid`	Process ID of the `named` process
`/var/tmp/named.run`	Debug output file
`/var/tmp/named_dump.db`	Dump of name server database
`/var/tmp/named.stats`	Nameserver statistics data

Configuration files will be owned by the BIND uid with a group owner of root, sys, or bin. The file permissions will be 640, or more restrictive, except for `resolv.conf`, which will be 644 to make it readable for all accounts. Only the IAO will authorize system(s) to be DNS servers. If a system is not authorized by the IAO to be a DNS server, the SA will ensure all DNS software and/or daemons (`named`, `in.named`, etc.) will be disabled or the software removed from the system. DNS will be allowed only on dedicated systems. A data base management system (DBMS) will be allowed if the DNS software supports it. DNS systems will not allow unnecessary network services. Disallowing unnecessary network services will help protect the system from unauthorized access, which could lead to compromise of systems and networks. Sites using BIND will upgrade to the newest version available for their system(s).

The ISC, www.isc.org, distributes the source for BIND. Different vendors distribute compiled BIND packages, sunfreeware.com, for instance. Find more information on `named` and BIND vulnerabilities at http://www.cert.org/advisories.

Some suggestions for implementing BIND are as follows:

1. BIND should be run as a non-privileged user for protection in the event of future remote compromise attacks (However, only processes running as root can be configured to use ports below 1024 [a requirement for DNS]). Therefore, configure BIND to change the userid after binding to the port.)

2. BIND should be run in a chroot(ed) directory structure for protection in the event of future remote compromise attacks.

3. Create Access Control Lists (ACLs) to restrict who can run recursive queries.

4. Restrict who can query root domain servers – this prevents a DNS server from being used as a DNS server for external sites that you are not supporting.

- *(G613: CAT II) The SA will ensure the configuration files (`/etc/named.boot`, `/etc/named.conf`, and the various DNS database files) have access permissions of 640, or more restrictive, and `the resolv.conf` file with permissions of 644.*

- *(G615: CAT II) The SA will ensure the configuration files (`/etc/resolv.conf`, `/etc/named.boot`, `/etc/named.conf`, and the various DNS database files) are owned by the uid of the BIND process, with a group owner of root, sys, or bin.*

- *(G617: CAT II) The IAO will ensure DNS is implemented only on dedicated hardware, with the exception that a DBMS may be implemented if the DNS system supports it.*

- *(G619: CAT II) The SA will ensure DNS software is disabled or removed from systems not dedicated as a DNS server.*

- *(G621: CAT I) The DNS administrator will ensure the minimum version of BIND installed is the DOD recommended version (available through IAVM alerts).*

4.22 Instant Messaging (IM)

Instant Messaging or IM clients provide a way for a user to send a message to one or more other users in real time. Additional capabilities may include file transfer and support for distributed game playing. Communication between clients and associated directory services are managed through messaging servers. Commercial IM clients include AOL Instant Messenger (AIM), MSN Messenger, and Yahoo! Messenger.

IM clients present a security issue when the clients route messages through public servers. The obvious implication is that potentially sensitive information could be intercepted or altered in the course of transmission. This same issue is associated with the use of public e-mail servers. In order to reduce the potential for disclosure of sensitive Government information and to ensure the validity of official government information, IM clients that connect to public instant messaging services will not be installed. Clients used to access an internal or DOD controlled IM applications are permitted.

- *(G623: CAT II) The SA will ensure that public instant messaging clients are not installed.*

- *(G625: CAT II) The SA will ensure instant messaging clients that are used for an internal or DOD controlled IM applications are at the current patch level.*

4.23 Peer-to-Peer File-Sharing Utilities and Clients

File sharing utilities and clients can provide the ability to share files with other users (Peer-to-Peer Sharing). This type of utility is a security risk due to the potential risk of loss of sensitive data and the broadcast of the existence of a computer to others. There are also many legal issues associated with these types of utilities including copyright infringement and intellectual property issues.

Per ASD Memo, Use of Peer-to-Peer (P2P) File-Sharing Applications across the DOD:

“P2P file-sharing applications are authorized for use on DOD networks with approval by the appropriate Designated Approval Authority (DAA). Documented requirements, security architecture, configuration management process, and a training program for users are all requirements within the approval process. The unauthorized use of application or services, including P2P applications, is prohibited, and such applications or services must be eliminated.”

P2P applications include, but not limited to the following:

- Napster
- Kazaa
- ARES
- Limewire
- IRC Chat Relay
- BitTorrent

- *(G627: CAT II) The SA will ensure that peer-to-peer file-sharing applications are not installed unless authorized and documented with the DAA.*

4.24 Samba

Samba is a utility allowing file and printer sharing between UNIX and Microsoft Windows operating systems. UNIX systems use TCP/IP whereas Windows uses Server Message Block (SMB) for sharing files. Windows shares files using the Common Internet Filesystem (CIFS). CIFS uses SMB and the Network Basic Input Output System (NetBIOS) interface to share network resources. Samba was created to provide an interface to give the look, feel, and functionality of Windows and enable UNIX systems to become part of a Windows domain, allowing file, directory, and printer sharing. If Windows sharing is not a requirement then the Samba utility should be removed or not installed. If the Samba utility is required, follow the security guidance provided below.

Samba is a suite of programs that use `/etc/samba/smb.conf` as the configuration file. The `smbd` daemon provides file and printer sharing, while `nmbd` provides NetBIOS name resolution and service browser support. Several utilities allow NFS-like access, mounting and unmounting of shared directories, and checking the status of the smb server. Samba includes an administration tool called the Samba Web Administration Tool (SWAT). It provides a GUI interface to configure the `/etc/samba/smb.conf` file through a web browser. When sharing network files and printers, access can be granted in two different ways, share mode and user mode. In share mode, one password is set for each shared resource and any user that knows the password can access it. In user mode, each user has an individual password that is stored in the `smbpasswd` file (which defaults to the `/etc` directory, but may be put anywhere depending on the `smb.conf` configuration).

Samba provides services, but there is some risk. SWAT runs as a service on port 901 by default, and requires a root logon to be accessed. If SWAT is used to administer Samba, it will be redirected through SSH, or a similar utility, to encrypt the root logon and Samba configuration data. The `/etc/samba/smb.conf` file will be owned by root, have a group owner of root, with permissions of 644, or more restrictive. The `smbpasswd` utility will be owned by root, with a group owner of root, with permissions of 644, or more restrictive. The `/etc/samba/smb.conf` file will be configured to allow access to systems on the local network, require the user access mode, password encryption, and have shares defined with guest set to `No`.

Samba is an add-on package avaible for most UNIX platforms, although, Linux provides this package as part of the default operating system platform.

- *(G629: CAT II) The SA will ensure* `smb` *is disabled, removed, or not installed if file sharing with Windows is not operationally required and implemented.*

- *(G631: CAT II) The SA will only use the Samba Web Administration Tool with SSH port forwarding.*

- *(G633: CAT II) The SA will ensure the owner of the* `/etc/samba/smb.conf` *file is root.*

- *(G635: CAT II) The SA will ensure the group owner of the* `/etc/samba/smb.conf` *file is root.*

- *(G637: CAT II) The SA will ensure the* `/etc/samba/smb.conf` *file has permissions of 644, or more restrictive.*

- *(G639: CAT II) The SA will ensure the owner of* `smbpasswd` *is root.*

- *(G641: CAT II) The SA will ensure group owner of* `smbpasswd` *is root.*

- *(G643: CAT II) The SA will configure permissions for* `smbpasswd` *to 755, or more restrictive.*

- *(G645: CAT II) The SA will configure the* `/etc/samba/smb.conf` *file to:*

  - *Set the hosts allow option to contain the local network subnet masks and the loopback address.*
  - *Set the security option to* `user`.
  - *Set the encrypt passwords option to* `Yes`.
  - *Enter the path to the* `smbpasswd` *utility in the smb* `password file` *option.*

- *(G647: CAT III) The SA will configure Samba to start automatically.*

4.25 Internet Network News (INN)

Internet Network News (INN) servers access Usenet news feeds and store news group articles. INN servers use the Network News Transfer Protocol (NNTP) to transfer information from the Usenet to the server and from the server to authorized remote hosts.

Several news servers are available for UNIX and Linux, and most distributions of Linux include at least one news server package. An Internet news server will not be loaded if there is no operational requirement. The `/etc/news/hosts.nntp` file will contain the list of authorized Usenet servers and have permissions of 600, or more restrictive, if there is an operational requirement. The `/etc/news/nnrp.access` file will contain the list of remote systems authorized for news access and have permissions of 600, or more restrictive. The `/etc/news/passwd.nntp` file will contain at least one password and have permissions of 600, or more restrictive. All configuration files will be owned by root or news, and have a group of root or news.

- *(G649: CAT II) The SA will disable all Internet news package files unless justified and documented with the IAO.*

- *(G651: CAT II) If NNTP is implemented, the SA will ensure the `/etc/news/hosts.nntp` file has permissions of 600, or more restrictive.*

- *(G653: CAT II) If NNTP is implemented, the SA will ensure the `/etc/news/hosts.nntp.nolimit` file has permissions of 600, or more restrictive.*

- *(G655: CAT II) If NNTP is implemented, the SA will ensure the `/etc/news/nnrp.access` file has permissions of 600, or more restrictive.*

- *(G657: CAT II) If NNTP is implemented, the SA will ensure the `/etc/news/passwd.nntp` file has permissions of 600, or more restrictive.*

- *(G659: CAT II) If NNTP is implemented, the SA will ensure the owner of all files under the `/etc/news` subdirectory is root or news.*

- *(G661: CAT II) If NNTP is implemented, the SA will ensure the group owner of all files in `/etc/news` is root or news.*

5. NETWORK BASED AUTHENTICATION

In the early days of computer use, all information necessary for an application was contained on storage media physically attached to the computer system on which the application executed. With the advent of networks and network technologies, many computer applications were designed to communicate with other computers to share information and to store data centrally. Initial communication protocols for sharing information did not consider authenticating requests for data or command execution. In turn, the confidentiality and integrity of data was not ensured. Today, computer information must be guarded to assure privacy and accuracy. This guarding is handled by assorted encryption schemes and protocols that establish trust relationships between two or more computers. Communication protocols also ensure end-to-end data integrity.

5.1 Network Information Service (NIS)

Network Information Service (NIS) is a database system that provides a mechanism for sharing network objects and resources. NIS provides a uniform storage and retrieval method for network-wide information in a transport-protocol and media-independent fashion.

NIS provides databases, called maps, to house name service data, including information such as user data, machine addresses and names, network and network services, mail, timezone, etc. NIS provides a centralized location for the SA to distribute and update maps among the NIS master and slave servers and NIS clients. This collection of network information is referred to as the NIS namespace.

NIS maps can only be updated by transferring an entire map to a slave. NIS uses no authentication between computers on a network. This poses a serious threat to security. NIS maps will be secured in such a way they cannot easily be obtained by a malicious user. The best way to do this is to make the NIS domain name hard to guess. NIS can be easily configured incorrectly. It has several well-known vulnerabilities, making it difficult to secure systems using NIS. For that reason and others, NIS should not be used. If NIS must be used, this will be justified and documented with the IAO.

- *(G663: CAT I) The SA will ensure NIS does not run under UDP.*

- *(G665: CAT II) The SA will ensure NIS is not used unless it is justified and documented with the IAO.*

- *(G667: CAT II) The SA will ensure NIS maps are protected through hard-to-guess domain names.*

5.2 Network Information Service Plus (NIS+)

Network Information Service Plus (NIS+) was designed to replace NIS. Like NIS, NIS+ is a distributed database system that allows a master server to share selected files with slave servers. These shared files are called NIS+ objects. NIS+ objects include password files, group files, and directory information. The files appear to be available on each computer, while in reality the files are resident on only the master server, or are replicated on database servers. The master is called the NIS+ root domain server. Workstations on the network, referred to as NIS+ principals, use the databases stored on the network as if they were being accessed locally.

Unlike NIS, NIS+ provides a level of security for the namespace and the information it stores by incorporating authorization and authentication. NIS+ authentication works by passing all communications between master and principal through a secure Remote Procedure Call (RPC) that encrypts the authentication session between the master and client, but does not encrypt the data that is transmitted. Every component in the namespace specifies the type of operation it will accept and from whom. NIS+ attempts to authenticate all access requests to the namespace. Access requests come from NIS+ principles. An NIS+ principal can be a process, machine, root, or a user. NIS+ credentials are used to authorize NIS+ principles. NIS+ authenticates the originator of the request by checking the originator's credential. NIS+ executes requests if there is a valid credential and the principal is authorized to perform the request. If the credential is invalid, or the request is not one the principal is authorized to perform, NIS+ denies the request for access.

NIS+ can operate in one of two security levels, 0 or 2. Security level 0 allows access by any NIS+ principals with full access to all NIS+ objects. Security level 2, the default, provides a higher level of security by authenticating principal requests using DES credentials.

- *(G669: CAT II) The SA will ensure the use of the Network Information Service, and NIS+ will be used as opposed to NIS, when available.*

- *(G671: CAT II) The SA will ensure NIS+ servers operate at security level 2 (the default level).*

6. UNIX SECURITY TOOLS

Security tools can generally be classified as vulnerability assessment, file system integrity checking, intrusion detection, and intrusion prevention (such as firewalls, proxy servers, honey pots). These tools provide enhanced security by allowing SAs to monitor and/or limit system and file access and modification. The SA must utilize vulnerability assessment and intrusion detection tools. Vulnerability assessment and intrusion detection tools generally operate with a flexible set of rules and policies and keep system baselines in a database. Some security tools require their databases to be online continuously; others do not. In some cases, such as with Tripwire, it is very easy to completely remove the application and the associated database files after they have been used, and reload them once a week when needed.

The mention of any particular tool within this section does not, in any way, suggest endorsement or approval. The tools mentioned within this section is mearly meant to provide some level of options. This is by no means an all-inclusive list. These are among many other options, as well, a site may develop homegrown tools that encompass the security requirements detailed within this *STIG*.

Whenever possible and practical (as with Tripwire databases), working copies of security tools and their database files should not be kept on the system. This will help protect against unauthorized database manipulation and program modification. When that is not possible, the programs and databases will be protected from unauthorized access by applying access permissions no more permissive than 740. Security tools and databases will be owned by a privileged uid and a privileged gid, or the COTS/GOTS default.

To ensure vulnerability assessment and intrusion detection is exercised, the IAO will develop Standard Operating Procedures (SOPs) to require intrusion detection on a continuous basis, and vulnerability assessment on a weekly basis. The SOP will also require the SA to provide all vulnerability assessment and intrusion detection reports to the IAO as soon as possible after the reports are available. All security reports will be retained in accordance with applicable Command regulations/directives. Any security incident detected by security tools will be reported and dealt with according to Command incident reporting procedures. The IAO will ensure security problems (not to be confused with security incidents) will be corrected as soon as possible. The SA will be responsible for documenting all actions to correct security tool findings in the system log and the IAO will review the log weekly.

- *(G673: CAT II) The SA and IAO will ensure a host-based intrusion detection tool is implemented.*

- *(G675: CAT II) The SA will ensure security tools and security files are owned by a privileged uid and gid.*

- *(G677: CAT II) The SA will ensure security tools and databases have permissions of 740, or more restrictive.*

- *(G679: CAT II) The SA will run vulnerability assessment tools at least weekly.*

- *(G681: CAT II) The SA will ensure methods used to check file integrity also notify the SA and the IAO via email if a security breach or a suspected security breach is discovered.*

6.1 Obtaining Security Tools

The site at https://sso.mont.disa.mil/prodsupport/utilities/index.html contains OpenSSH, OpenSSL, Sudo, TripWire, TCP Wrappers, and SSO Putty. This site does not require logon.

The CM site at https://sso-dads.mont.disa.mil contains some SSO-supported products for Tivoli, MQSeries, PCAnywhere, and Mercury Interactive Topaz products. It also contains SSO-developed UNIX and Windows Security Automation products. This site is UID controlled. To obtain a UID, select "New Users Enter Here" from the center of the page, select DD Form 2875, complete it, and follow the instructions on the page to submit it.

The site, http://www.cert.org/security-improvement/implementations/i042.07.html, which is maintained by Carnegie Mellon Software Engineering Institute, also maintains a comprehensive list of tools that aid in detecting suspicious behavior for the UNIX and Linux operating systems. Though not required, some of these tools can be utilized in fulfilling the UNIX security requirements.

6.2 Baseline/File System Integrity Tools

A file system integrity/baseline tool will take a baseline of all files, or a specific subset of files, to include cryptographic hashes of files in the baseline. The tool must be able to compare the baseline of the system against the current state of the system later so that unauthorized modification of the file system can be detected.

6.2.1 Symantec Enterprise Security Manager (ESM)

Symantec Enterprise Security Manager (ESM) is a client/server product that provides the capability to define and implement user policies to manage systems in an enterprise network. ESM scans the operating system, and detects and reports variations from user-defined policies. ESM includes the capabilities of CRACK and Tripwire.

6.2.2 Tripwire

Tripwire is a utility that checks file and directory integrity against a previous baseline database. Tripwire reports all differences including added or deleted entries it detects. When run against system files on a regular basis, Tripwire enables the detection of changes in critical system files and facilitates immediate damage control measures.

6.2.3 Automated Security Enhancement Tool (ASET)

Solaris includes the Automated Security Enhancement Tool (ASET), which monitors and controls system security. One of the many security features included within ASET is a baseline/file system vulnerability checking feature.

6.2.4 Basic Audit Reporting Tool (BART)

Solaris 10 includes the Basic Audit Reporting Tool (BART), which is a filesystem tracking tool. BART allows for the creation of baselines and additionally provides snapshot and reporting ability to easily check for any unwanted file changes.

6.2.5 Advanced Intrusion Detection Environment (AIDE)

Advanced Intrusion Detection Environment (AIDE) provides for creating a baseline database and checking the integrity of the file system.

6.2.6 FCheck

FCheck is an open source PERL script providing intrusion detection and file system integrity checking through the use of comparative system snapshots. FCheck provides monitoring and notifications of any file modifications, additions, and deletions.

6.2.7 Symantec Symantec Intruder Alert (ITA)

Symantec Intruder Alert (ITA) provides intrusion detection by monitoring system logs and audit files. ITA will generate notification of possible intrusions using electronic mail, beepers, or screen messages. It can also be programmed to initiate defensive action, such as terminating a logon process, disabling accounts, and disabling tty devices.

6.3 Host-Base Intrustion Detection Tools

6.3.1 FCheck

FCheck is an open source PERL script providing intrusion detection and file system integrity checking through the use of comparative system snapshots. Fcheck provides monitoring and notifications of any file modifications, additions, and deletions.

6.3.2 Symantec Intruder Alert (ITA)

Symantec Intruder Alert (ITA) provides intrusion detection by monitoring system logs and audit files. ITA will generate notification of possible intrusions using electronic mail, beepers, or screen messages. It can also be programmed to initiate defensive action, such as terminating a logon process, disabling accounts, and disabling tty devices.

6.4 Vulnerability Assessment Tools

Vulnerability assessment tools will aide in the indentification of security weaknesses. These tools can scan UNIX platforms and notify the SA of possible security issues.

- CyberCop
- Enterprise Inspector
- Internet Scanner
- SAINT
- Retina

6.5 Password Checking Tools

6.5.1 Computer Oracle and Password System (COPS)

Computer Oracle and Password System (COPS) includes many features, including security checks related to file permissions and modes, format of password and group files, anonymous ftp configuration, and weak passwords to name a few.

6.5.2 CRACK

Crack is a classic UNIX password-cracking tool.

6.5.3 John the Ripper

John the Ripper is a fast password-cracking tool with a primary purpose to detect weak UNIX passwords.

6.6 Access Control Programs and TCP_WRAPPERS

The Transmission Control Protocol/Internet Protocol (TCP/IP) wrapper program provides an IP filtering capability and additional network logging information. It gives a SA the ability to deny or allow access from certain systems or domains to the host on which the program is installed. The IAO and the SA should work together to ensure access to their systems is restricted to authorized systems, domains, and networks. TCP_WRAPPERS uses `hosts.allow` and `hosts.deny` files to accomplish this. Hosts can be allowed access to only certain network services while being denied access to all others. TCP_WRAPPERS provides a good method of restricting access to systems and of detecting unauthorized access attempts through its logging and notification capability. TCP_WRAPPERS also provides the capability to display messages prior to a logon attempt. For that reason, it is the preferred method of displaying system-warning banners. It offers much more functionality than other programs, such as `klaxon`, that claim to detect port scans.

- *(G683: CAT II) The SA will ensure an access control program (e.g., TCP_WRAPPERS) is implemented on all UNIX hosts connected to a network.*

- *(G685: CAT II) The SA will ensure an access control program (e.g., TCP_WRAPPERS) is configured to log each system access attempt.*

- *(G687: CAT II) The SA will ensure an access control program (e.g., TCP_WRAPPERS)* `hosts.deny` *and* `hosts.allow` *files (or equivalent) are used to grant or deny system access to specific hosts.*

6.7 System Hardening

6.7.1 Bastille

The Bastille Hardening System is a set of scripts that, when run on a Linux system, increase the security (also called hardening) of many of the configurations. The application walks the SA through several modules, and automates changing a large number of configurable system items. Bastille has modules for checking and configuring Internet services, suid (set-user-ID) files, account and boot security, and TCP_WRAPPERS.

FSO has not subjected the Bastille Hardening System to acceptance testing. It is presently not available from a trusted source. If the SA chooses to use the Bastille utilities, the SA should use only the latest version of the product, remove the system from the network before execution, and execute a complete system backup. After use, as a precaution, the SA will verify that the changes selected were implemented and they were the only changes implemented and there were no security vulnerabilities introduced. The SA will perform a self-assessment after using Bastille, by running the UNIX scripts and noting deficiencies. The Bastille Hardening System program is available from http://www.bastille-linux.org/. Bastille currently supports:

- Red Hat (Fedora Core, Enterprise, and Numbered/Classic)
- SuSE
- Debian
- Gentoo
- Mandrake
- HP-UX

6.8 Auditing

6.8.1 System iNtrusion Analysis & Reporting Environment (SNARE)

System iNtrusion Analysis & Reporting Environment (SNARE) provides an auditing and logging system for Linux.

This page is intentionally left blank.

7. SYSTEM BACKUPS

Please see *Section 2.5.4, Backup and Recovery,* of the *Enclave STIG* for operating system backup and recovery guidance and requirements.

This page is intentionally left blank.

8. SUN SOLARIS

Although general UNIX considerations are covered in the initial sections of this document, this section addresses several Solaris specific items. Solaris 10 has many advantages in regards to security, including compliance with password history and account lockout capabilities. These are two requirements, which until Solaris 10, Solaris could not incorporate without add-on tools or configuration of PAM modules. *Section 8.8, Solaris 10*, provides an overview of the security enhancements provided within this release of Solaris.

8.1 Removable Media

The `nosuid` option will be configured on removable media to prevent suid programs being copied or moved onto the system.

- *(SO03: CAT II) The SA will ensure the `nosuid` option is configured in the `/etc/rmmount.conf` file.*

8.2 The audit_user File

The `/etc/security/audit_user` file is an access-restricted audit configuration file for customizing per-user auditing flags. The file is used to change the auditing level for specific users without changing the system-wide auditing defaults. Vendors supply the file populated with an entry for root. The SA will remove this entry and ensure the `audit_user` file never contains flags that diminish the level of auditing for any user, including root and other system accounts. The owner of the file will be root and group owner of the file will be root, sys, or bin. The file will not be accessible by any but privileged accounts and should have file permissions of 640, or more restrictive.

- *(SO05: CAT II) The SA and IAO will ensure the `audit_user` file will not be used to diminish the level of auditing for any user, including root and other system accounts.*

- *(SO07: CAT II) The SA will ensure the owner of the `audit_user` file is root.*

- *(SO09: CAT II) The SA will ensure the group owner of the `audit_user` file root, sys, or bin.*

- *(SO11: CAT II) The SA will ensure the `audit_user` file has permissions are 640, or more restrictive.*

8.3 Automated Security Enhancement Tool (ASET)

ASET is designed to help the SA monitor and control system security. It can be set to operate at one of three security levels (low, medium, or high). These security levels restrict the permission settings for ASET identified objects.

- *(SO13: CAT II) The SA will ensure the ASET master files (`tune.high`, `tune.low`, `tune.med`, and `uid_aliases`) are located in the `/usr/aset/masters` directory.*

8.3.1 The uid_aliases File

The `uid_aliases` file contains a list of user accounts sharing the same username. ASET warns about any such multiple user accounts.

- *(SO15: CAT III) The SA will ensure the `/usr/aset/masters/uid_aliases` file has no entries.*

8.3.2 The asetenv File

The environment file `/usr/aset/asetenv` contains a list of variables that affect ASET tasks and has two main sections—a user-configurable parameters section and an internal environment variables section.

- *(SO17: CAT II) The SA will ensure if the UNIX computer system is used as a firewall, the user-configurable parameters section of the `/usr/aset/asetenv` file will be set up to run as a firewall.*

- *(SO19: CAT II) The SA will ensure the following shell environment variables are defined as indicated:*

```
CKLISTPATH_LOW=${ASETDIR}/tasks:${ASETDIR}  \
/util:${ASETDIR}/masters:/etc
CKLISTPATH_MED=${CKLISTPATH_LOW};/usr/bin:/usr/ucb
CKLISTPATH_HIGH=${CKLISTPATH_MED}:/usr/lib:/sbin:  \
/usr/sbin:/usr/ucblib
PERIODIC_SCHEDULE="0 0 * * *" (NOTE: A daily run.)
UID_ALIASES=${ASETDIR}/masters/uid_aliases
```

8.3.3 Running ASET

YPCHECK environment variable specifies whether ASET should also check system configuration file tables. YPCHECK is a Boolean variable; only `true` or `false` may be specified. The default value is `false`, which disables NIS+ table checking. When set to `false`, ASET checks the local `passwd` file. When set to `true`, the task also checks the NIS+ `passwd` table for the domain of the system. The `userlist` file will have any entry for each user on the system. ASET will perform environment checkst on each user listed within the `userlist` file. The file name is specified with the `–u userlist_file` parameter, a different file name may be specified; this is to be taken into consideration.

- *(SO21: CAT II) The SA will ensure, if using ASET and NIS+ is running, YPCHECK will be set to `true`.*

- *(SO23: CAT II) The SA will ensure a list of all users on a system are kept in a file called `/usr/aset/userlist`. The `userlist` file will contain one user per line.*

- *(SO25: CAT II) The SA will ensure the owner of the `/usr/aset/userlist` file is root.*

- *(SO27: CAT II) The SA will ensure the`/usr/aset/userlist` file has permissions of 600, or more restrictive.*

8.4 The Electrically Erasable Programmable Read-only Memory (EEPROM) Command

The Electrically Erasable Programmable Read-only Memory (EEPROM) command displays or changes the values of parameters in the EEPROM. It is possible to restrict who can bring the system to single-user mode by requiring a password for EEPROM.

The EEPROM Security Mode will be set to `command` or `full`. Auto-boot should be set to `false` if the system is not located in a restricted access area. Auto-boot should be set to `true` if the system is in a restricted access area and it is desired the system reboot itself automatically if power is lost and restored. The EEPROM security password will be set using existing password guidelines. The EEPROM password will be protected. The EEPROM password will not be the same as the root password. This will allow an operator to boot the system without needing to know the root password. The EEPROM monitor will provide a logon banner. Since it cannot be as extensive as the operating system level banner, a suggested banner is: “DOD use only! Subject to monitoring, reporting, and prosecution.” The oem-banner will be set to `true` to ensure the banner is displayed when the EEPROM monitor is logged on to.

- *(SO29: CAT II) The SA will ensure the EEPROM contains a logon warning banner.*

- *(SO31: CAT II) The SA will ensure the EEPROM Security-mode is `command` or `full`.*

- *(SO33: CAT II) The SA will ensure the EEPROM password is set using STIG standards.*

- *(SO35: CAT III) The SA will ensure the EEPROM password is not the same as the root password.*

8.5 Sun Answerbook2

Sun AnswerBook2 is a utility that allows users to view Sun documentation using a Web browser.

8.5.1 Script Access

A vulnerability regarding the lack of authentication in AnswerBook2, versions 1.2 through 1.4.2 could allow a remote attacker to gain unauthorized access to administrative scripts. This would allow the attacker to perform administrative functions, such as creating a new admin user or view the server's error log.

Suns AnswerBook 2 utilizes a third-party web server daemon (`dwhttpd`) that suffers from a format string vulnerability. The vulnerability can be exploited to cause the web server process to execute arbitrary code. The web server runs as user and group, daemon. The user, daemon, under recent installations of Solaris, owns no critical files. Typically, daemon only owns all files pertaining to the AnswerBook 2 installation. This effectively limits the severity of the vulnerability to a remote unprivileged shell.

In addition, not all AnswerBook Admin scripts require authentication, allowing the attacker to perform administrative functions without an account. Among other things, it is possible to add a new admin user or view the server's error log.

The combination of these two vulnerabilities allows for a remote exploit that can determine the exact location of its payload, requiring no guessing of return addresses or NOP padding.

- *(SO37: CAT II) The SA will ensure the Sun Answerbook2 does not allow unauthorized script access.*

8.5.2 dwhttpd Format String

By default, AnswerBook2 installs a third-party web server daemon, Inso DynaWeb Web server (`dwhttpd`), to display the online documentation. AnswerBook2 versions 1.2 through 1.4.2 are vulnerable to a format string vulnerability in the `dwhttpd` daemon. A remote attacker can exploit this vulnerability by supplying an overly long input string of hexadecimal encoded characters as a file name in a specially crafted GET request to execute code on the system with daemon privileges.

- *(SO39: CAT II) The SA will ensure the Sun Answerbook2 is not vulnerable to the `dwhttpd` format string vulnerability.*

8.6 Snoop

Solaris continues to integrate snoop with their software distributions. The snoop utility allows privileged users to snoop network traffic and possibly capture and inspect data and passwords that are passed in the clear. Snoop is not normally usable by unprivileged users, but can be used to gain much knowledge if a privileged password is compromised. There are few legitimate uses for snoop. Therefore, snoop will be deleted.

- *(SO41: CAT II) The SA will ensure the snoop utility does not exist.*

8.7 NFS Server Logging

NFS server logging enables an NFS server to provide a record of file operations that are performed on its filesystems. This feature is particularly useful for sites that make anonymous FTP archives available to NFS and WebNFSTM clients.

- *(SO43: CAT II) The IAO will ensure NFS server logging is implemented on NFS servers.*

8.8 Solaris 10

Of the many features provided with Solaris 10, below listed are a few related to security and performance.

- Password History
- Disable account after failed login attempts
- BART, discussed in *Section 6.2.4, Basic Audit Reporting Tool (BART)*
- N1 Grid Containers – Allows for a server to be divided to appear as several machines
- Increased TCP/IP networking processing
- NextGen file system, to allow for 128-bit addressing schemes to accommodate exabyte size data
- Predictive self-healing monitors and detects memory problems

8.8.1 Root Default Group

Prior to Solaris 10, the group for the root account is other; Solaris 10 is configured with root's default group as root. This is another security step to prevent unauthorized access to root owned files.

- *(SO45: CAT I) The SA will ensure only root has the gid of 0 (root).*

This page is intentionally left blank.

9. HEWLETT PACKARD UNIX (HP-UX)

Although general UNIX considerations are covered in the initial sections of this document, this section addresses several HP-UX specific items.

9.1 Trusted Mode

HP refers to the use of its C2 level software as running in trusted mode. Trusted mode is a requirement and it can be implemented using the HP System Administration Manager (SAM). When trusted mode is configured, it also enables the auditing capability. Auditing can then be configured using SAM.

- *(HP03: CAT II) The IAO will ensure all HP-UX systems are configured to operate in trusted mode.*

9.1.1 Trusted System Auditing

Besides the standard HP-UX auditing features, a system that has been configured to run in trusted mode enables an SA to track user activities by the system calls they evoke. Tunable auditing parameters and events are located in `/etc/rc.config.d/auditing`. The default primary audit log file is `/.secure/etc/audfile1`. Also, during the system conversion to trusted mode, the process creates audit ID numbers for all users to enable specific tracking of user activities.

- *(HP05: CAT II) The SA will ensure the `AUDOMON_ARGS` flag is set to the following:*

  - *`fss` is set to a minimum of 20 percent (`-p 20`). `fss` is the minimum percentage of free space left on an audit log file's filesystem before switching to the secondary audit log file.*

  - *`sp_freq` is set to a maximum of one minute (`-t 1`). `sp_freq` is the time interval within which warning messages about the switch points are generated and sent to the console.*

  - *`warning` is set to a maximum of 90 percent (`-w 90`). `warning` is the percentage of audit file space used or minimum free space used, after which warning messages are sent to the console.*

9.2 The /etc/securetty File

HP-UX restricts direct root logon via the `/etc/securetty` file. The IAO will ensure the file exists, has permissions of 640, or more restrictive, is owned by root, and has a group owner of root.

- *(HP07: CAT II) The SA will ensure the owner of the `/etc/securetty` file is root.*

- *(HP09: CAT II) The SA will ensure the group owner of the `/etc/securetty` file is root, sys, or bin.*

- *(HP11: CAT II) The SA will ensure the `/etc/securetty` file has permissions of 640, or more restrictive.*

10. IBM ADVANCED INTERACTIVE EXECUTIVE (AIX)

Although general UNIX considerations are covered in the initial sections of this document, this section addresses several AIX specific items.

10.1 Security Structure

AIX implements a Trusted Computing Base (TCB) to comply with the C2 security level. The TCB regulates access to system resources by acting as the interface between the user and the AIX kernel.

- *(AIX03: CAT II) The IAO will ensure the TCB module is installed and implemented.*

10.2 Network Security

Some TCP/IP commands and daemons are nontrusted and lack the ability for required I&A, these are as follows:

- rcp
- rlogin
- rlogind
- rsh
- rshd
- tftp
- tftpd

The AIX command `securetcpip` provides enhanced security by disabling these commands and daemons. These are not deleted, but disabled by changing the mode to 0000.

SSH is a much more secure option. SSH communicates using encryption to protect data and passwords. It provides strong authentication and secure communications over insecure channels. SSH also provides `rlogin`, `rsh`, `rcp`, and `rdist` services, but since the communications are encrypted, it is done in a much more secure manner than traditional services.

- *(AIX05: CAT II) The SA will ensure the `securetcpip` command is used.*

10.3 System Commands

Shell scripts cannot run suid. Only binary commands may have the suid bit set. This feature of AIX limits the security exposure.

AIX provides a command, `chtcb`, for root's use to set a special TCB bit in a program's inode. This bit, when set, signifies the trusted kernel may execute the program.

- *(AIX07: CAT II) The SA will ensure the TCB bit baseline file is compared with the online TCB bit files on a weekly basis.*

11. SILICON GRAPHICS (SGI) IRIX

Although general UNIX considerations are covered in the initial sections of this document, this section addresses several IRIX specific items.

11.1 Xfsmd

The `xfsmd` daemon in SGI IRIX versions 6.2 through 6.5.x is installed and running by default. A vulnerability regarding the lack of filtering for shell metacharacters in the `popen()` function (`xfsmd`) could allow a remote attacker to embed arbitrary commands in user-supplied arguments to the `popen()` function to execute arbitrary commands on the system with root privileges.

- *(IRIX03: CAT I) The SA will ensure the Xfsmd is not enabled.*

11.2 Programmable Read-Only Memory (PROM)

The Command (Programmable Read-Only Memory [PROM]) Monitor provides access to IRIX system hardware. This can allow unauthorized users to boot the system with an unauthorized program, remove hardware, or install hardware. The SA will ensure the Command (PROM) Monitor is password protected. The Command (PROM) Monitor security password will be set using existing password guidelines. The Command (PROM) Monitor password will be protected. The Command (PROM) Monitor password will not be the same as the root password.

- *(IRIX05: CAT II) The SA will ensure the Command (PROM) Monitor is password protected.*

- *(IRIX07: CAT II) The SA will ensure the Command (PROM) Monitor password is set using STIG standards.*

- *(IRIX09: CAT III) The SA will ensure the Command (PROM) Monitor password is not the same as the root password.*

This page is intentionally left blank.

12. LINUX

Although general UNIX considerations are covered in the initial sections of this document, this section addresses several Linux specific items. This section is for all Linux variants, but guidance is based on Version 6.2 through 9.0 of Red Hat Linux and version 9.0 of SuSE Linux. Based on the variant of Linux, file names, directory paths, variable names, etc., may have to be taken into consideration.

There are comments on other versions of Linux, such as Mandrake, Caldera and the new United Linux, etc., whenever it is appropriate. There are numerous versions of Linux and it would be beyond the scope of this *STIG* to try to detail them all. Please note, all requirements listed within this section will pertain to all versions of Linux unless explicitly noted otherwise.

12.1 Processing Environment

Linux was designed, at first, to run on x86 systems. It migrated to larger systems such as Sun Scalable Processor Architecture (SPARC), and the IBM mainframe. It competes favorably (though the numbers are not as large) with Microsoft Windows for the personal computer (PC) market. As of this writing, the only distributions of Linux to be included on the NIAP Validated Products List for Common Criteria are as follows:

- Red Hat Enterprise Linux 3 EAL2
- Red Hat Enterprise Linux AS, Version 3 Update 2 EAL3
- Red Hat Enterprise Linux WS, Version 3 Update 2 EAL3
- Red Hat Enterprise Linux AS, Version 3 Update 3 EAL3
- Red Hat Enterprise Linux WS, Version 3 Update 3 EAL3
- SuSE Linux Enterprise Server V8 EAL2
- SuSE Linux Enterprise Server V8, Service Pack 3, RC4 EAL3+

Reference *Section 1, Introduction,* of this *STIG* for additional information on NIAP evaluation requirements and product endorsement.

12.2 System BIOS Configuration

The more common hardware platform for a Linux system is a PC. PCs use a Basic Input Output System (BIOS) contained in a programmable complimentary metal-oxide semiconductor (CMOS). The CMOS contains the machine instructions needed to bring the system to the point the operating system can be loaded (i.e., booted). When the SA is configuring the CMOS after initial configuration, the CMOS will be set to disable booting from other than the hard disk. The reasons for setting a BIOS password are to prevent accidental or malicious tampering with BIOS settings and to prevent booting from other media. If the BIOS password is not set and a malicious user or intruder obtains physical access to the system, it is possible to boot the system to single-user mode or to boot from a CDROM or diskette. The root shell runs when in single user mode. Root can be gained by booting from diskette or CDROM. An intruder has compromised the system once access to root is obtained.

- *(L001: CAT II) The SA will set the CMOS password for x86 systems.*

- *(L003: CAT I) The SA will edit the CMOS settings to disable the capability to boot from removable media.*

12.3 Restricting the Boot Process

As in *Section12.2, System BIOS Configuration,* boot options will be set to prevent booting from a floppy disk. This operation will vary from computer to computer, based on the manufacturer's specifications. Assuming use of an x86 system during the initial boot sequence, the prompt 'Press FX to enter setup' is displayed. (FX is used here as an example. Some systems use F2, Ctrl/Del, or Ctrl/Esc. Check the system's operating manual for specific details.) The SA will set the Password Configuration Table with the `Supervisor Password ON` and the `User Password OFF`.

- *(L005: CAT II) The SA will set the Password Configuration table with the `Supervisor Password ON` and the `User Password OFF`.*

12.4 Boot Loaders

The boot loader runs the operating system when the system is powered up or rebooted. There are four options for boot loaders:

1. GRUB Console Loader
2. Linux Loader (LILO)
3. A third party loader
4. No loader at all

If a boot loader was not chosen, a boot disk would have to be created and would open the system to being booted from any boot disk. The SA will configure Linux systems to use a boot loader. That leaves the GRUB Console, LILO, or a third party loader. The boot loader must support journaling filesystem types and encrypt the boot loader password. If the boot loader does not support these requirements, for example, a vendor proprietary configuration, this will be justified and documented with the IAO.

- *(L007: CAT I) The SA will not implement a boot diskette as a boot loader.*

- *(L009: CAT I) The SA will only configure the GRUB Console as the boot loader or a boot loader, such as current releases of LILO, that supports journaling filesystem types and the boot loader password can be encrypted. If the boot loader does not support these requirements (for example a vendor proprietary configuration), the host is to be located in a controlled access area accessible only by SAs and this will be justified and documented with the IAO.*

12.4.1 Boot Loader Passwords

The reasons for password protecting boot loader passwords are to prevent access to;

1. Single User Mode. This allows root level access.

2. The boot loader. This allows the capability to view and/or modify hardware information.

3. Non-Secure Operating Systems. If a dual-boot system, possibly allows booting from un-authorized operating systems.

12.4.1.1 Password Protecting the GRUB Console Boot Loader

The GRUB Console boot loader must be password protected to avoid the possibility of maliciously booting to a single user mode, or booting an insecure operating system. The permissions of the `grub.conf` file will be 600.

- *(L011: CAT I) The SA will configure the GRUB Console Boot Loader with a MD5 encrypted password.*

- *(L013: CAT II) The SA will ensure the `grub.conf` file has permissions of 600, or more restrictive.*

12.4.1.2 Password Protecting the LILO Boot Loader

LILO is a simpler boot loader and does not offer a command interface, so there is no danger of an attacker gaining control of the system before it is loaded. It must still be password protected to avoid the possibility of maliciously booting to a single user mode, or booting an insecure operating system. The permissions of the lilo`.conf` file will be 600.

- *(L015: CAT I) The SA will ensure the global password is configured in the `lilo.conf` file.*

- *(L017: CAT I) The SA will encrypt the LILO boot loader password.*

- *(L019: CAT II) The SA will ensure the `lilo.conf` file has permissions of 600 or more restrictive, if it exists.*

12.5 Filesystems

Filesystem journaling provides a system with its own backup and recover capability. Prior to any disk writes, the data changes are first recorded to a log, and then written to disk. Journaling will commit a change to the log or can roll back in a transactional manner. Journaling provides for more stable filesystems and stronger data integrity by ensuring no loss of data after unclean system crashes and shutdowns. A journaled filesystem will be used on all primary Linux filesystems.

- *(L021: CAT II) The SA will configure a journaling filesystem on the primary Linux filesystem partitions (if this is not supported). This will be justified and documented with the IAO.*

12.6 Logical Volume Manager (LVM) for Linux 8 and 9

Red Hat Linux 8.0 introduced the Logical Volume Manager (LVM) for hard drive space flexibility. LVM is a way to allocate hard drive space into logical volumes that can be easily resized, instead of using inflexible partitions. With LVM, the hard drive, or set of hard drives (such as a Redundant Array of Independent Disks – RAID), is allocated into one or more physical volumes. A physical volume is not able to span over more than one drive. Physical volumes are combined into logical volume groups. An exception is the `/boot` partition, which may not reside on a logical volume group because the boot loader is not able to read it. If the root partition is needed on a logical volume, a separate boot partition not part of a volume group must be created. Since a physical volume is not able to span over more than one drive, if it is desirable for logical volume groups to span over more than one drive, then one or more physical volumes per drive must be created. Logical volume groups are divided into logical volumes. Logical volumes are assigned mount points such as `/home` and `/`. They are also assigned filesystem types, such as ext3. When partitions are full, space from the logical volume group can be added, thus increasing the size of the partition and avoiding a repartition of the disk drive or filesystem. One great advantage of the LVM is that logical volumes, that are the partitions, can be expanded. On the other hand, if a system is partitioned with the ext3 filesystem, the hard drive is divided into partitions of defined sizes. If a partition becomes full, it is not easy to expand the size of the partition. Even if the partition is moved to another hard drive, the original hard drive space has to be reallocated as a different partition or not used. LVM support must be compiled into the kernel by default for Red Hat Linux 8.0.

- *(L023: CAT I) The IAO will not allow the boot partition to reside on removable media unless it is stored in a secure container (safe) to be used in emergencies only.*

12.7 Red Hat Kickstart and SuSE AutoYaST

Newer Red Hat Linux versions have a utility to automate installation called Kickstart. SuSE Linux supplies a similar product with the same functionality called AutoYaST. An SA can create a file with the answers, one on each line, to all the questions that would normally be asked while installing Linux. The Kickstart/Auto YaST files can be kept on one server and read by many clients to achieve installation standardization. This installation method leaves the machines exposed to attack prior to and during the installation process. Kickstart and Auto YaST will only be used to configure systems connected to an isolated development LAN with no outside network connections. Upon completion of the installation process and implementation of DOD security standards and requirements, the system(s) may be incorporated into the production environment.

- *(L025: CAT I) The SA will ensure Kickstart and Auto YaST are used only on an isolated development LAN.*

12.8 Dual Boot

Linux can co-exist with other operating systems, such as Windows, on the same physical medium. Many Linux distributions provide a boot manager and can read File Allocation Table (FAT), FAT32, and New Technology Filesystem (NTFS) partitions. This ability allows Linux applications to access information on those partition types. The information could be sensitive. This flexibility creates risks to systems with multiple operating systems where the systems, other than Linux, are not aware of and take heed to the capability. In some instances, it could be very useful. In other instances, it could be very harmful. The possibility of harmful consequences outweighs the good. Linux systems will not be allowed to contain more than one operating system unless the IAO is provided with justification and documentation from the proponents of the alternate 0perating system(s).

- *(L027: CAT II) The SA will configure the system to boot only Linux unless justified and documented with the IAO.*

12.9 Ugidd RPC Daemon

The `ugidd` daemon is used on older Linux systems to map uids and gids that may differ from the NFS server to the NFS client. The `ugidd` daemon could allow a remote attacker to list all the users on specific systems. If installed on the machine, it will not be used.

- *(L033: CAT II) The SA will ensure the `ugidd` daemon is not enabled.*

12.10 Default Accounts

Several accounts are created by default during the standard Linux install process. Default system accounts are normally listed at the beginning of the `/etc/passwd` file and have names like bin, lib, uucp, news, sys, guest, and daemon. Some of the accounts (e.g., shutdown and halt) may allow access to system administration tasks without giving the operator, for instance, the root password. Others provide no operational purpose (such as games and operator). These accounts (including shutdown and halt) will be removed from the system before it is connected to the network.

- *(L035: CAT I) The SA will delete accounts that provide a special privilege such as shutdown and halt.*

- *(L037: CAT II) The SA will delete accounts that provide no operational purpose, such as games or operator, and will delete the associated software.*

12.11 X Windows

Linux uses Xfree86 in place of the proprietary X Windows System found in UNIX, but the functionality and configuration is almost identical.

- *(L041: CAT II) The SA will enable the X server* `–audit` *(at level 4) and* `–s` *option (with 15 minutes as the timeout time) options.*

- *(L043: CAT II) The SA will disable the X server* `–ac, -core`*, and* `-nolock` *options.*

12.12 Console Access

Linux provides an additional layer of security by allowing for restricting console login access. Depending on the version of Linux, the file used to restrict access is `/etc/login.access` or `/etc/security/access.conf`. The `/etc/login.access or /etc/security/access.conf` file will be owned by root, have a privileged group, and have permissions of 640, or more restrictive. The `/etc/login.access` or `/etc/security/access.conf` file will contain entries to allow access only from the system console by authorized SAs.

- *(L047: CAT II) The SA will ensure the owner of the* `/etc/login.access` *or* `/etc/security/access.conf` *file is root.*

- *(L049: CAT II) The SA will ensure the group owner of the* `/etc/login.access` *or* `/etc/security/access.conf` *file is root.*

- *(L051: CAT II) The SA will ensure*`/etc/login.access` *or* `/etc/security/access.conf` *file will be 640, or more restrictive.*

- *(L053: CAT II) The SA will ensure `/etc/login.access` or `/etc/security/access.conf` will contain entries restricting console access to authorized SAs only.*

12.13 Kernel Configuration File

Network parameters are configured in `/etc/sysctl.conf`, which is the kernel configuration file. The `/etc/sysctl.conf` file will be owned by root, have a group owner of root, and permissions set at 600.

- *(L055: CAT II) The SA will ensure the owner of the `/etc/sysctl.conf` file is root.*

- *(L057: CAT II) The SA will ensure the group owner of the `/etc/sysctl.conf` file is root.*

- *(L059: CAT II) The SA will ensure the `/etc/sysctl.conf` file has permissions of 600, or more restrictive.*

12.14 NFS Server

By default NFS exports with the `secure` option set. The `secure` option configures NFS to run on a reserved port (i.e., ports 1-1024). This ensures non-root users cannot open a spoofed NFS dialogue on a non-reserved port.

By default NFS exports with the `secure_locks` option set. Please note this setting is for older Linux releases and may not apply. The `secure_locks` option ensures user permissions are checked prior to file access.

- *(L061: CAT I) The SA will ensure the `insecure` option is not set.*

- *(L063: CAT I) The SA will ensure the `insecure_locks` option is not set.*

12.15 The /etc/inittab File

The `/etc/inittab` file controls the initial boot level as well as processes and daemons started within each boot level. The SA will disable the Ctrl-Alt-Delete functionality if the system is not located in a controlled access area.

- *(L065: CAT I) The SA will disable the Ctrl-Alt-Delete sequence unless the system is located in a controlled access area.*

12.16 Pluggable Authentication Module (PAM) Authorization File

The configuration file for PAM is `/etc/pam.d/system-auth`. The PAM configuration file contains generic authentication requirements. The configuration tool is authconfig. Manual modification to the `/etc/pam.d/system-auth` file will be overwritten when the authconfig tool is used. The following entries are required to enable the password restrictions referenced earlier.

```
auth required /lib/security/pam_env.so
auth required /lib/security/pam_tally.so onerr=fail
no_magic_root
auth sufficient /lib/security/pam_unix.so likeauth nullok
auth required /lib/security/pam_deny.so
account required /lib/security/pam_unix.so
account required /lib/security/pam_tally.so deny=3
no_magic_root reset
password required /lib/security/pam_cracklib.so retry=3
minlen=8 lcredit=-1 ucredit=-1 password sufficient
/lib/security/pam_unix.so nullok use_authtok md5 shadow
remember=15
password required /lib/security/pam_deny.so
session required /lib/security/pam_limits.so
session required /lib/security/pam_unix.so
```

12.17 Administrative Controls

A PAM module, `pam_console.so`, allows some activities normally reserved only for the root user, such as rebooting and mounting removable media to the first user that logs in at the physical console. This method will not be used because it could deny legitimate root access (using the `su` command) from another terminal.

- *(L067: CAT II) The SA will not configure the PAM configuration file to allow the first person to log in at the console sole access to certain administrative privileges.*

12.18 The /etc/securetty File

Linux restricts direct root logon via the `/etc/securetty` file. The SA will ensure the file has permissions of 640, or more restrictive, is owned by root, with a group owner of root.

- *(L069: CAT II) The SA will ensure the group owner of the `/etc/securetty` file is root, sys, or bin.*

- *(L071: CAT II) The SA will ensure the owner of the `/etc/securetty` file is root.*

- *(L073: CAT II) The SA will ensure the `/etc/securetty` file has permissions of 640, or more restrictive.*

12.19 RealPlayer

SUSE Linux includes RealPlayer as both standalone player and as a plugin for web browsers like Mozilla and Konqueror. RealPlayer may also be downloaded and installed on most Linux platform. This might allow the attacker to just provide a web page or E-Mail linking to the special exploit .rm file.

Affected SuSE versions;

- SUSE Linux versions up to 9.1 and the SUSE Linux Desktop 1.0 include RealPlayer version 8.

- SUSE Linux 9.2 and the Novell Linux Desktop 9 include RealPlayer version 10 and are NOT affected.

- *(L075: CAT II) The SA will ensureRealPlayer version 8 is removed from SuSE 9.1 and SuSE Linux Desktop 1.0.*

This page is intentionally left blank.

13. WORLD WIDE WEB SERVER SERVICES AND PROTOCOLS

Guidance for World Wide Web server services and protocols may be found in the *Web Server STIG*.

This page is intentionally left blank.

14. SYSTEMS HOSTING DATABASE APPLICATIONS

Guidance for systems hosting database applications may be found in the *Database STIG*.

This page is intentionally left blank.

15. MQSERIES 5.2

MQSeries is a message transmission utility developed by International Business Machines (IBM). MQSeries provides applications the ability to communicate with each other across multiple platforms using messages and queues. MQSeries runs on multiple platforms (e.g., MVS, UNIX, NT, Tandem, etc.) and uses multiple protocols (e.g., TCP, UDP, LU 6.2). It is a client/server suite. A system can be configured to run the client version of the software, the server version of the software or both at the same time. MQSeries removes an applications need to address network protocol requirements and different platform requirements while transferring data. An application is provided with a standard set of MQ APIs which when used perform the transmission of data.

MQSeries uses messages and queues to perform data transfer. Whenever an application is expected to transmit data using MQSeries, it calls an MQSeries queue manager. The queue manager takes the data and converts it into message format and stores it in the queue it manages. When the message is ready to be transferred, the queue manager passes the message to the transmit queue and notifies the Message Channel Agent (MCA) the message is ready for transmission. The sending MCA passes the message up the channel to the receiving MCA's queue and notifies the receiving MCA the message is available. The receiving MCA then notifies the receiving queue manager and the message is transferred to the receiving queue manager's queue. The receiving queue manager notifies the receiving application the message is ready and transfers the message back into its original form. The application is then able to take the file and process it. Responses are then sent back the same way.

15.1 General Considerations

MQSeries provides a mechanism for assigning access authority to administrators using an Object Authority Manager (OAM). Other security must be provided through user-supplied exit programs. There is no built-in mechanism to provide data encryption for messages (queries and/or updates) except through user-supplied message exits. Native security (such as UNIX file ownership, assigned access permissions, etc.) also provides security for the MQSeries directory/file structures when properly maintained.

15.2 Installing MQSeries

MQSeries, though easy to install, has several prerequisites for installation. Careful planning for disk layout and user authority assignments is necessary. The IAO should work closely with the SA to plan for user and system access authority, and should document all decisions. The SA will be most conversant with the options that exist to increase disk access efficiency and to protect system filesystems. A good deal of disk space may be conserved by installing only the language options that are necessary for the locale.

15.2.1 Prior to Installing

Prior to installing MQSeries, create a user account called mqm and a UNIX group called mqm. The home directory for mqm will be `/var/mqm`. Follow password guidelines for assigning a password to mqm, or disable the account using a false shell and locking the password. MQSeries administrators are required to be a member of the mqm group. The root user must also be a part of the mqm group. Choose members of the mqm group carefully, since all members of the mqm group have administrative authority in MQSeries. The IAO will approve, justify, and document all mqm group members. The IAO will approve, justify, and document all group/user authorizations that are assigned through other means, such as the OAM. Other installations should use a method that is familiar to them. In the absence of a comprehensive method, FSO can supply one.

- *(MQ01: CAT II) The IAO will ensure all recommended patches have been installed.*
- *(MQ02: CAT II) The SA will ensure the /var/mqm, or mqm home directory, permissions are no more permissive than 770.*
- *(N/A: CAT III) The IAO will approve, justify, and appropriately document all mqm group members.*
- *(N/A: CAT III) The IAO will approve, justify, and appropriately document MQSeries access authority granted through other means (such as the OAM).*

FSO recommends installing MQSeries on newly installed/reinstalled operating systems. The SA will ensure all vendor-recommended patches are installed before installing MQSeries. This can be checked by downloading the recommended patches from the vendor and using the `swlist` command (HP-UX) or the `patchinfo -p` command (Solaris) to compare installed patches with the recommended list. The IAO will ensure each system is STIG compliant before and after MQSeries is installed.

Mount the installation CD-ROM, and read the README file that pertains to the particular system. Acquire and install any additional patches listed in the README file. Follow the other installation directions in the *Quick Beginnings* manual supplied with the code for the particular system and MQSeries version.

IBM recommends that separate filesystems be created for `/var/mqm/log` and `/var/mqm/errors`. The installation will work without separate filesystems if the system has ample disk space. The reasons for the recommendation are to increase access efficiency and to help protect other data if the logs and/or error logs become voluminous enough to fill the `/var` filesystem, thus adversely affecting data availability and data integrity.

Allow a minimum of 30 MB (megabytes) of storage for `/var/mqm`, two MB of storage for `/var/mqm/errors`, and 20 MB of storage for `/var/mqm/log` if using separate filesystems. If installing them on a single filesystem, allow at least 52 MB.

15.2.2 Installation Procedures

The system's native software installation manager will be used to install MQSeries. Check this by verifying the software can be identified with the `swlist` command (HP-UX) or the `patchinfo –p` command (Solaris). On HP systems, the software installation manager is `swinstall`. On Sun systems, the software installation manager is `pkgadd`. On AIX systems, the software installation manager is `xinstallm` (use the `-ez` parameter). For Digital UNIX systems, use the `setld -l` command.

The IBM installation procedures provide ample file and directory access protections except for the `/var/mqm/errors` and `/var/mqm/trace` directories. The permissions for these directories will be changed to 775, or more restrictive. The errors and trace directories and logs also exist for each queue manager, and these access permissions should be changed to correspond with these requirements. MQSeries files and directories will be owned by the mqm account.

Log files that exist under each queue manager are created with a protection of 666. These should be changed to 660, or more restrictive, unless justified and documented with the IAM and IAO. The group owner of MQSeries files and directories will be the mqm group. Security exit programs that access the TCB file structure may have sys as a group owner and be setgid to sys. Write permissions will not be granted to other for any MQSeries file or directory unless justified and documented with the IAO.

- *(N/A: CAT III) The SA will use the native installation manager to install MQSeries.*

- *(N/A: CAT II) The SA will ensure MQSeries files and directories are owned by the mqm account.*

- *(N/A: CAT II) The SA will ensure the group owner of MQSeries files and directories is the mqm group, except for certain exit programs for which the group owner may be the sys group.*

- *(N/A: CAT II) Write permissions will not be granted to other for any MQSeries file or directory.*

- *(N/A: CAT III) The SA will ensure write permissions are not granted to any other MQSeries file or directory unless justified and documented with the IAO.*

The `/var/mqm/errors` and `/var/mqm/trace` directories may be NFS mounted to conserve space on the local system. NFS exported and mounted filesystems are subject to the same requirements as for other systems.

15.3 MQSeries Logs

MQSeries has the capability to log errors and transaction activity. The logging of errors and transaction activity will be implemented. MQSeries can be configured to use circular or linear logs. A circular log will log data into the log file until the file reaches a predefined size, and will then start over at the beginning of the file, destroying previous data. A linear log will continue until cleaned out by the administrator. Sites will use linear logs. Logs will be backed up daily. The size of the log file depends upon the log settings and type of logs (linear or circular). Access to the logs will be limited to the mqm account, the mqm group, certain applications, and certain utilities.

- *(MQ03: CATII) The SA will ensure the /var/mqm/log directory has permissions of 770 or more restrictive.*

- *(MQ04: CAT II) The IAO and SA will ensure neither the /var/mqm directory nor the /var/mqm/log directory is NFS mounted.*

- *(MQ05: CAT III) The SA will ensure transaction logging is implemented.*

- *(MQ06: CAT II) The SA will ensure linear logs are used.*

- *(MQ07: CAT II) The SA will limit access to MQSeries logs to members of the mqm group, MQSeries applications, and MQSeries utilities.*

- *(MQ32: CAT II) The SA will ensure error logging is performed.*

- *(N/A: CAT III) The SA will ensure logs are backed up daily.*

15.4 Authorization Directories

The default authorization directories are under the following default paths:

```
/var/mqm/qmgrs/system-name/queues
/var/mqm/qmgrs/system-name/proc-def
/var/mqm/qmgrs/system-name/qmanager
/var/mqm/qmgrs/system-name/namelist
```

These authorization files will have access permissions no more permissive than 660. The directories will have access permissions no more permissive than 770. All will be owned by mqm with a group owner of mqm.

- *(MQ08: CAT II) The SA will ensure authorization directories and files are owned by mqm.*

- *(MQ09: CAT II) The SA will ensure authorization directories and files have a group owner of mqm.*

- *(MQ10: CAT II) The SA will ensure authorization file permissions are 660, or more restrictive.*

- *(MQ11: CAT II) The SA will ensure authorization directory permissions will be* 770*, or more restrictive.*

15.5 Kernel Configuration

Each UNIX system is supplied with a default kernel configuration. MQSeries uses semaphores and shared memory, and the default configuration for UNIX kernels is not adequate to fully support it. The default kernel values must be increased and the kernel recompiled. This is not a trivial task. System kernel parameters (e.g., `shmmni`, `semmni`, `semmns`, and `semmnu`) need to allow for the number of queue managers in the system. The following sections contain the IBM recommended kernel values for the listed systems. The values shown may need to be increased if any First Failure Support Technology (TM) (FFST[TM]) records are generated in the logs.

15.5.1 Solaris 2.5.1 Kernel Parameters

```
set shmsys:shminfo_shmmax = 4194304
set shmsys:shminfo_shmseg = 1024
set shmsys:shminfo_shmmni = 1024
set shmsys:shminfo_shmem = 1
set semsys:seminfo_sema = 1
set semsys:seminfo_semaem = 16384
set semsys:seminfo_semvmx = 32767
set semsys:seminfo_semmni = 1024
set semsys:seminfo_semmap = 1026
set semsys:seminfo_semmns = 16384
set semsys:seminfo_semmsl = 100
set semsys:seminfo_semopm = 100
set semsys:seminfo_semmnu = 2048
set semsys:seminfo_semume = 256
set msgsys:msginfo_msgmni = 50
set msgsys:msginfo_msgmap = 1026
set msgsys:msginfo_msgmax = 4096
set msgsys:msginfo_msgmnb = 4096
set msgsys:msginfo_msgssz = 8
set msgsys:msginfo_msgtql = 40
set msgsys:msginfo_msgseg = 1024
set maxusers = 32
```

Review the Solaris 2.5.1 installation by using the `sysdef -i` command. To change the values, add a `set parameter = value` line to the `/etc/system` file.

15.5.2 HP/UX 10.X Kernel Parameters

```
shmmax          4194304
shmseg          1024
shmmni          1024
shmem           1
sema            1
semaem          16384
semvmx          32767
semmns          16384
semmni          1024
semmap          1026
semmnu          2048
semume          256
msgmni          50
msgtql          256
msgmap          258
msgmax          4096
msgmnb          4096
msgssz          8
msgseg          1024
maxusers        32
```

Review the HP/UX installation by using the sysdef command. To change the values, use the SAM utility.

15.5.3 SCO 5.X Kernel Parameters

For normal operation of the MQSeries system, the Kernel parameters for STREAMS may need to be increased from the default values. A value as large as 524,288 bytes may be required for the STRMAXBLK parameter, depending on the system configuration.

15.5.4 Digital UNIX Kernel Parameters

Review the machine's configuration and increase the values if necessary after the installation.

```
ipc:
  sem-mni=4096
  sem-msl=1000
  sem-opm=100
  sem-ume=1000
  shm-mni=4104
  shm-seg=1024
  num-of-sems=3000
  shm-max=2147483647
```

Kernel parameter values must be placed in the `/etc/sysconfigtab` file. IBM recommends using the `dxkernel tuner` for the operation.

15.6 Channel Security Exits

MQSeries provides a distributed queuing environment. Channel security exits will be implemented to provide authentication between the MCAs on a channel. The exits must authenticate with a unique Message Queue Identification (MQID) (system or host ID) and password for each channel. The channel security exits work in pairs. To work properly, the exits must use the same protocol to pass data to both ends of the channel pair. MQSeries expects to find exits in the `/var/mqm/exits` directory, by default.

The MQSeries default directory for exits can be changed by editing the `/var/mqm/mqs.ini` file and changing the `ClientExitPath` stanza to read something other than `ExitsDefaultPath=/var/mqm/exits`.

To change the default directory for exits for specific queue managers, edit the configuration file for the queue manager. It is located in the `/var/mqm/qmgrs/qmname/qm.ini` file (where `qmname` is your name for the queue manager). Change the `ExitPath` stanza to something other than `ExitsDefaultPath=/var/mqm/exits`. The defaults provide the easiest way to configure MQSeries, however. The IAO will approve and document any variation from the standard default exit program locations.

All exit programs will be reviewed for security and approved by FSO. An exit is a routine in the main body of code (MBC – MQSeries) that looks for user-written programs configured with specific names and in specific locations. The MBC exits to the supplied program, or exit routine. The exit routine performs its function (e.g., checking the user identification and password of the system attempting to connect), and sends a status code to the MBC when it is finished. The exit program may also break the channel connection if the user identification (system identification) and password pair does not match the access list. The MBC proceeds based on the status code returned from the exit routine.

On UNIX systems, as on other systems, exits can present a security problem if not properly protected. The MBC does not care what is there, only that it is there. Therefore, all exit programs will have access permissions of 770, or more restrictive. Channel security exits that must access the Hewlett Packard Trusted Computing Base (TCB) file structure provide an exception to this rule. Exit programs may be assigned a group owner of sys, may be setgid to sys, and may be assigned permissions of 2770. Exit programs will be owned by the mqm account and have a group owner of mqm, except as outlined above.

Exceptions (such as making an exit suid to some other ID) will be granted by FSO and approved by the local IAO and IAM on a case-by-case basis. Exits will exist in directories that are readable and writable only by the mqm userid and the mqm group (except as outlined above). Access permissions will be 770, or more restrictive.

It should be noted that installations running version 5.2 use CommerceQuest's Enablenet Data Integrator (DI) and ProtectMQ. Both products together are designed to provide secure file transfer. When messages are sent across the MQSeries channels, the ProtectMQ message exits intercept and encrypt them on the outbound side and decrypt them on the inbound side. ProtectMQ and DI also handle PKI processing. In order to use DI and ProtectMQ changes will have to be made involving adding additional objects through OAM. The changes involve adding DI queues and the ProtectMQ security exit `libmqsec` instead of specifying the GOTs exit.

- *(MQ12: CAT II) The IAM will ensure FSO approves all exit programs.*

- *(MQ13: CAT II) The SA will ensure exit program access permissions are 770, or more restrictive, unless approved and documented with the IAO and IAM, except in the case where the exit has to access the Hewlett Packard Trusted Computing Base. The permissions may be 2770 in this case.*

- *(MQ14: CAT II) The SA will ensure all exit programs are owned by mqm.*

- *(MQ15: CAT II) The SA will ensure exit programs have a group owner of mqm. The exception will be in the case of channel security exits, which must access the Hewlett Packard Trusted Computing Base (TCB) file structure. It may have a group owner of sys.*

- *(MQ23: CAT III) The IAO, application developer, and Program Manager will ensure data encryption is used.*

- *(MQ33: CAT II) Developers, the IAO, and the SA will ensure all exit programs are placed in the default `/var/mqm/exits` directory unless approved by and documented with the IAO and IAM. An exception is for MQSeries 5.2 when the use of the CommerceQuest Enablenet Data Integrator (DI) and ProtectMQ are approved for use in place of the GOTS/COTS exits.*

15.7 Configuration Files

The MQSeries configuration files are `mqs.ini` and `qm.ini`. The `mqs.ini` file is a global configuration file that defines MQSeries resources for the node. The `qm.ini` file is the configuration definition for the queue manager. Each `qm.ini` file defines the configuration of a single queue manager. There may be multiple `qm.ini` files based on the number of queue managers. The access permissions for configuration files will be 660. If the owner and group owner for `mqs.ini` and `qm.ini` files is not mqm, then the IAO will maintain documentation justifying the aberration.

- *(MQ16: CAT II) The SA will ensure access permissions for the MQSeries configuration files are 660, or more restrictive.*

- *(MQ17: CAT II) The SA will ensure the owner of the MQSeries configuration files is mqm, unless documented with the IAO.*

- *(MQ18: CAT II) The SA will ensure the group owner of the MQSeries configuration files is mqm, unless documented with the IAO.*

15.8 Dead Letter Queues

When a message cannot reach its destination, the channel queue will be stopped unless a Dead Letter Queue (DLQ) has been defined for each queue manager on the system. Every queue manager in a network will have an associated local DLQ defined. A default DLQ is supplied with the installation and is called `SYSTEM.DEAD.LETTER.QUEUE`, but that is not enough. Create additional DLQs using the `crtmqm` command or the `ALTER QMGR` command for each queue manager.

Two levels of access must be defined for DLQs. Use the OAM to accomplish this. The first level allows applications, etc. to `PUT` messages to the queue. The second level restricts the ability to `GET` messages from the queue and protects sensitive data. The two levels are implemented with the use of an alias queue that resolves to the DLQ. The alias queue is defined with the attributes `PUT(ENABLED)` and `GET(DISABLED)`. The ability to `GET` will be restricted to message channel agents, channel initiator utilities, and any automated application used for DLQ maintenance.

The following describes how to securely define a DLQ:

1. Define the real DLQ with attributes `PUT(ENABLED)` and `GET(ENABLED)`.

2. Give update authority, using the OAM command `setmqaut`, to the mqm group, channel initiators, and any automated applications used for DLQ maintenance.

3. Define an alias queue, from within the `runmqsc` program, that resolves to the real DLQ, but give the alias queue the attributes `PUT(ENABLED)` and `GET(DISABLED)`.

4. Give the userid associated with the application update authority, using the OAM command `setmqaut`, for the alias queue, but no access to the real DLQ.

- *(MQ19: CAT II) The SA will ensure a Dead Letter Queue is defined for each queue manager in the network.*

- *(MQ20: CAT II) The SA will ensure Dead Letter Queues are defined for security.*

- *(N/A: CAT II) The SA will ensure the ability to GET is restricted to message channel agents, channel initiator utilities, and any automated application used for DLQ maintenance.*

15.9 Security

MQSeries provides an interface for including a user identifier (i.e., a queue manager ID, a host ID, or an actual userid) and an associated password with each message. Native UNIX system security and user-developed security exit programs are the only other security features. Message headers, therefore, will contain the identification of the sending queue manager. Security exits will be written to verify the source of each message. MQSeries does not provide encryption services. Therefore, message exits should be written to provide end-to-end data encryption and decryption services for each message. An alternate technique may be encryption between firewalls, but this is not true end-to-end encryption. The encryption technique should be based on a minimum 128-bit key.

IBM supplies then OAM that is installed by default with UNIX systems unless the installer specifies otherwise. The OAM manages user authorizations to manipulate MQSeries objects including queues and process definitions. It provides a command-line interface, and can be used to grant or revoke access authority to an object for a specific group of users. The SA will ensure OAM is installed with all MQSeries installations. Authorization for using MQI calls, commands, and access to objects can be provided or reset by the OAM, which by default is enabled. MQSeries entities are controlled through UNIX groups (such as mqm) and the OAM. A command-line interface is provided to enable administrators to grant or revoke authorizations as required.

- *(MQ22: CAT I) Security exit developers will ensure security exits are written to provide the sending queue manager identification and authorization.*

- *(MQ24: CAT III) The SA will ensure the OAM is installed and enabled/implemented with all MQSeries installations.*

- *(N/A: CAT II) Developers, IAOs and SAs will ensure MQM message headers contain the identity of the sending queue manager.*

15.10 Userid Timeouts

Userids signed on to a queue manager will be logged off after 15 minutes of inactivity. This is a universal requirement that should be implemented in MQSeries.

15.11 Connection Security

Connection security validates userids authorized to connect to queue managers. Connection security will be implemented. Connection authority will be authorized, justified, and documented with the IAO. Channel security exits will be used to maintain connection security. MQSeries systems should use TCP_WRAPPERS, or a similar utility, to maintain system access control.

- *(MQ25: CAT II) Application developers will ensure connection security is implemented through channel security exits.*

- *(N/A: CAT III) Application developers and Program Managers will ensure connection authority is authorized, justified, and documented with the IAO.*

15.12 Queue Security

Queue security validates userids (and system IDs) authorized to access message queues. Queue security will be implemented. Message queue access will be restricted to those userids that require the ability to get messages from, and put messages to, message queues. Access authorization to system queues will be restricted to utilities, MQSeries operations and control panels, channel initiators, and actual transactions. Queue access will be authorized, justified, and documented with the IAO using *DISA Form 41*, where appropriate, and other documentation when *DISA Form 41* is not appropriate. Queue security will be implemented using the OAM to grant access rights on a granular basis to individual users and groups. Queue security will also be implemented through native UNIX security mechanisms and the use of channel security exits.

- *(MQ21: CAT II) The SA will ensure queue access is authorized, justified, and documented with the IAO.*

- *(MQ26: CAT II) The SA will ensure queue security is implemented by restricting access and authority through the OAM, through native UNIX security mechanisms, and through channel security exits.*

15.13 Process Security

Process security validates userids authorized to issue MQSeries inquiries on process definitions. A process definition object defines an application that is started in response to a trigger event on a queue manager. Process security will be implemented. Access to process definition objects will be justified, authorized, and documented by the IAO. Restrict *read* access to those userids requiring access to make process inquiries. Process security will be maintained, insofar as possible, through the OAM and through native UNIX security mechanisms.

- *(MQ27 CAT II) The SA will ensure process security is implemented using the native UNIX file and directory access permissions and through access and authorization assignments using the OAM.*

- *(N/A: CAT III) The SA will ensure inquiries to process definition objects are authorized, justified, and documented by the IAO.*

15.14 Namelist Security

An example of a namelist is an MQSeries object that contains a list of queue names. Namelist security validates userids authorized to inquire on namelists. Namelist security will be implemented. Access to namelists will be justified, authorized, and documented by the IAO. Restrict access to those userids requiring access to make namelist inquiries. Namelist security will be maintained through the native UNIX security mechanisms and, insofar as possible, through the OAM.

- *(MQ28: CAT II) The SA will ensure namelist security is implemented, insofar as possible, through the OAM and the native UNIX security mechanisms.*

- *(N/A: CAT III) The IAO will ensure access to namelists is authorized, justified, and documented.*

15.15 Alternate Userid Security

Alternate userid security allows access to be requested under another userid. Alternate userid security will be implemented. Access to alternate userids will be justified, authorized, and documented by the IAO.

- *(N/A: CAT II) The SA will ensure alternate userid security is implemented.*

- *(N/A: CAT III) The IAO will authorize, justify, and document access to alternate userids.*

15.16 Context Security

Context security validates whether or not a userid has the authority to pass or set identity and/or origin data for a message. Context security will be implemented through security exits. FSO will justify and authorize security exits. The IAO will document their use.

- *(MQ30: CAT II) The SA will ensure context security is implemented through security exits.*

- *(N/A: CAT III) The IAO will maintain documentation for all security exits.*

15.17 Command Security

Command security validates userids authorized to issue MQSeries commands. Command security will be implemented by UNIX access controls. The UNIX mechanism that can enforce command security is to ensure all MQSeries commands are owned by the mqm account and are group owned by the mqm group. The commands will have permissions no more permissive than 770, unless documented and justified with the IAO and IAM. All who require access to the MQSeries commands will be members of the mqm group.

- *(MQ31: CAT II) The SA will ensure command security is implemented through required UNIX access controls.*

15.18 MQSeries Commands

MQSeries provides the following three command sets for UNIX:

Control commands
MQSC commands
PCF commands

The following is a list of MQSeries MQSC commands with the recommended command access list. The MSCQ commands can be invoked using the `runmqsc` control command.

`ALTER`	MQ Admin., Sys. Progs., Queue Managers
`ARCHIVE LOG`	MQ Admin., Sys. Progs., Queue Managers
`CLEAR QLOCAL`	MQ Admin., Sys. Progs., Queue Managers
`DEFINE`	MQ Admin., Sys. Progs., Queue Managers
`DELETE`	MQ Admin., Sys. Progs., Queue Managers
`DISPLAY`	Appl. Progs., MQ Admin, Sys. Progs., Queue Managers
`PING`	Appl. Progs., MQ Admin, Sys. Progs., Queue Managers
`RECOVER BSDS`	MQ Admin., Sys. Progs., Queue Managers
`REFRESH`	Security staff, MQ Admin., Sys. Progs., Queue Managers
`RESET`	MQ Admin., Sys. Progs., Queue Managers
`RESOLVE`	MQ Admin., Sys. Progs., Queue Managers
`RESUME QMGR`	MQ Admin., Sys. Progs., Queue Managers
`RVERIFY SECURITY`	Security Staff, MQ Admin.
`START`	MQ Admin., Sys. Progs., Queue Managers
`STOP`	MQ Admin., Sys. Progs., Queue Managers
`SUSPEND QMGR`	MQ Admin., Sys. Progs., Queue Managers

The available control commands are issued from the UNIX command line. They entail OAM commands. The basic OAM commands are `dspmqaut` (display MQSeries authorizations) and `setmqaut` (set MQSeries authorizations). They are as follows:

`crtmqcvx`	-	Data conversion
`crtmqm`	-	Create queue manager
`dltmqm`	-	Delete queue manager
`dmpmqlog`	-	Dump log
`dspmqaut`	-	Displays authorizations to a specified object
`dspmqcsv`	-	Display command server
`dspmqfls`	-	Display MQSeries files
`dspmqtrn`	-	Display MQSeries transactions
`endmqcsv`	-	End command server
`endmqm`	-	End queue manager
`rcdmqimg`	-	Record media image
`rcrmqobj`	-	Recreate an object from images contained in the log
`rsvmqtrn`	-	Resolve MQSeries transactions
`runmqchi`	-	Run channel initiator
`runmqchl`	-	Run channel
`runmqdlq`	-	Run dead letter queue handler
`runmqlsr`	-	Run listener
`runmqsc`	-	Run MQSeries MQSC commands
`runmqtmc`	-	Start client trigger monitor
`runmqtrm`	-	Start trigger monitor
`setmqaut`	-	Set or reset authority
`strmqcsv`	-	Start command server
`strmqm`	-	Start queue manager

Programmable Command Format (PCF) commands allow administrative tasks to be programmed into an administration program. They cover the same range of functions provided by the MQSC facility, but the commands are in a slightly different format. They are described fully in the *MQSeries Programmable System Management* manual. PCF commands can be used to write programs to administer multiple nodes.

15.19 WebSphere MQ 5.3

WebSphere MQ, is the new version of MQSeries. WebSphere MQ is an IBM software product that provides applications the ability to communicate with each other across multiple platforms using messages and queues. WebSphere MQ provides the same functionality as MQSeries but was enhanced to handle security and PKI.

15.20 WebSphere MQ Exits

There are six types of WebSphere MQ exits that can be used to customizing channels. They range from security to message reformatting. Earlier releases of WebSphere MQ transferred data across channels in clear text. In order to secure WebSphere MQ message headers, a GOTs security exit was developed to encrypt the header information and to invoke the ACP on the mainframe.

WebSphere MQ uses SSL as the protocol for handling message transmission and performs security checking. In addition, WebSphere MQ allows for the use of PKI certificates to further enhance security. A function of SSL is to provide for the encryption and decryption of the entire message as it is transferred across the channel by the WebSphere MQ MCA. As a result, the use of a GOTs security exit between two WebSphere MQ 5.3 sites is not needed. In order to make use of SSL under WebSphere MQ, additional values will be supplied to the channel definition describing SSL usage. This information can be found in the IBM quick beginnings manual.

If a WebSphere MQ exit is developed, it must be submitted to DISA FSO FSO for a Program Integrity Analysis. Once approved by FSO, the exit can be used.

- *(N/A: CAT I) The SA will ensure WebSphere MQ channels are using SSL.*
- *(N/A: CAT I) The SA will ensure WebSphere MQ is using PKI certificates and they are stored in a key ring in the ACP database.*
- *(N/A: CAT IV) The SA will ensure DOD PKI certificates are used.*
- *(N/A: CAT I) The SA will ensure earlier releases of MQSeries are using a GOTs exit or CommerceQuest's EnableNet Data Integrator/MQProtect.*

15.21 WebSphere MQ Clustering

A WebSphere MQ cluster is a network of queue managers that are logically grouped to support an application. The queue managers in a cluster normally communicate directly with each other through automatically defined cluster channels. Every queue manager in a cluster is able to make their queues they host available to every other queue manager in the cluster. When a cluster is created, multiple queue managers are designated to be the full repository queue managers. These queue managers are responsible for storing information about the names of the queue managers and the network connections used by each.

Every queue manager in a cluster has a single transmission queue from which it can transmit messages to any other queue manager in the cluster. Whenever a message is to be sent across a cluster, the message is placed in the cluster transmission queue of the sending queue manager and is transmitted to all other queue managers in the cluster. Any queue manager can send the message to any other queue manager without the need for explicit channel definitions, remote-queue definitions, or transmission queues for each destination.

In order for a queue manager to become a member of a cluster, a cluster sender channel and a cluster receiver channel must be defined. The cluster sender channel points to the full repository queue manager. The cluster receiver channel provides the connection details. The name of the cluster sender channel must match the name of the cluster receiver channel on the full repository queue manager.

Three new system queue objects have also been introduced to support clustering. They are:

1. The queue, `SYSTEM.CLUSTER.TRANSMIT.QUEUE.`, is used to hold all messages that are ready to be sent to any queue manager in the cluster.

2. The queue, SYSTEM`.CLUSTER.COMMAND.QUEUE`, is used to exchange repository information.

3. The queue, `SYSTEM.CLUSTER.REPOSITORY.QUEUE`, holds the repository information as a number of persistent messages.

- *(N/A: CAT II) The IAO will ensure all cluster queue managers and queues are restricted to authorized systems and users.*

- *(N/A: CAT II) The IAO will ensure any security exit programs used on cluster channels are approved by FSO.*

15.22 Secure Sockets Layer (SSL)

Under WebSphere MQ 5.3, SSL is used to provide channel security. SSL is an industry-standard protocol that provides a data security layer between application protocols and the communications layer, usually TCP/IP. SSL uses encryption techniques, digital signatures and digital certificates to provide message privacy, message integrity and mutual authentication between clients and servers.

To use the Secure Sockets Layer (SSL) for channel security, do the following:

1. Create a key ring in the ACP to hold all the keys and certificates for the system. The id should be the channel initiator address space.

2. Create a digital certificate for each queue manager. The label of the certificate must be of the form `ibmWebSphereMQqmgr-name`.

3. Connect the certificate and any relevant signer certificates to the key ring in the ACP.

4. Point the queue manager to the key repository using the WebSphere MQ `ALTER QMGR` command.

5. Create an AUTHINFO object of AUTHTYPE CRLLDAP, using the WebSphere MQ DEFINE AUTHINFO command to indicate the Certificate Revocation Lists (CRLs) are stored on a specific LDAP server.

6. Set each queue manager to run SSL calls using the WebSphere MQ ALTER QMGR command. There must be at least two of these subtasks.

7. Specify the cipher specification for the channel on each end of the channel using the WebSphere MQ DEFINE CHANNEL or ALTER CHANNEL command.

- *(N/A: CAT I) The SA will ensure WebSphere MQ messages are encrypted using at a minimum DES2 encryption.*

- *(N/A: CAT I) The SA will ensure the WebSphere MQ channels use SSL.*

- *(N/A: CAT IV) The SA will ensure DOD approved certificates are stored in the ACP database.*

- *(N/A: CAT IV) The SA will ensure Certificate Revocation Lists (CRLs) are stored on a LDAP server that is restricted to authorized users.*

This page is intentionally left blank.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

DOD CIO Memo, Open Source Software (OSS) in Department of Defense (DOD), 28 May 2003.

Department of Defense CSC-STD-002-85, “DOD Password Management Guideline,” 12 April 1985.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, “Security Requirements for Automated Information Systems (AIS),” July 1996.

Defense Information Systems Agency Instruction (DISAI) 630-255-7, “Internet, Intranet, and World Wide Web,” September 1996.

Defense Information Systems Agency (DISA) Western Hemisphere (WESTHEM) Naming Convention Standards, February 1996.

Defense Information Systems Agency (DISA) Computing Services Security Handbook, Version 3, 1 December 2000.

Defense Information Systems Agency (DISA) Western Hemisphere (WESTHEM) Security Instruction 360-225-08, “Magnetic Tape Backup and Storage by Defense Megacenters,” November 1997.

Defense Information Systems Agency (DISA) OS/390 Security Technical Implementation Guide, Version 4, Release 1 (2 volumes), 4 August 2003.

Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide, Version 5, Release 3, 19 August 2003.

Defense Information Systems Agency (DISA) Web Server Security Technical Implementation Guide, Version 4, Release 1, 29 August 2003.

Department of Defense (DOD) Instruction Number 8500.2, 6 February 2003, Subject: Information Assurance (IA) Implementation.

DOD Directive 8500.1 (DOD), "Information Assurance" 24 October 2002.

DOD instruction 8500.2 (DOD), "Information Assurance (IA) Implementation" 06 February 2003.

DOD 5025.1-M (DOD), "DOD Directives System Procedures," current edition.

National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, "National Information Systems Security Glossary," September 2000.

DOD Directive 8000.1 (DOD), "Management of DOD Information Resources and Information Technology," 27 February 2002.

Addendum to the NSA Guide to Securing Microsoft Windows NT Networks and NSA Guides to Securing Windows 2000, Version 43 (to match NSA Guide), Release 1, 26 November 2002.

Developer's Guide for Using Mobile Code Technologies in Department of Defense and Intelligence Community Information Systems.

MQSeries System Administration (Second Edition, March 1999).

MQSeries Planning Guide (8th Edition, January 1999).

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 October 1991.

Army Regulation (AR) 380-19, "Information Systems Security," 1 August 1990.

Air Force Systems Security Instruction (AFSSI) 5100, "The Air Force Computer Security (COMPUSEC) Program," 2 June 1992.

Air Force Systems Security Memorandum (AFSSM) 5007, "A Methodology for Addressing DOD-Mandated "C2 by 92" for Operational Air Force Systems," 25 March 1991.

Secretary of the Navy Instruction (SECNAVINST) 5239.2, "Department of the Navy Automated Information Systems (AIS) Security Program," 15 November 1989.

Navy Staff Office Publication (NAVSO Pub) 5239-15, "Controlled Access Protection Guidebook," August 1992.

Public Law 100-235, 100th Congress, an Act cited as the "Computer Security Act of 1987," 8 January 1988.

Santa Cruz Operation, Inc.

SCO Open Desktop/SCO Open Server System Administrator's Guide - Operating System, Networking, and DOS Services (includes Performance and Troubleshooting)

Sun Microsystems, Inc.

Security, Performance, and Accounting Administration
SunShield Basic Security Module Guide
SunOS Reference Manual (*Section 1M, System Administration Commands*)

Hewlett-Packard

Using HP-UX
System Administration Tasks
Using the X Window System

International Business Machines, Inc**.**

AIX Version 4.3 System Management Guide: Operating System and Devices

Other

Anonymous. *Maximum Linux Security*, 2000, Sams Publishing.

Clyde, Robert A., et al. 1994. *Raxco Security Directives Series, UNIX Standards and Guidelines.* Rockville, MD: Raxco and Company.

Garfinkel, Simon, and Gene Spafford. 1991 and 1994. *Practical UNIX Security.* Sebastopol, CA: O'Reilly and Associates, Inc.

Kirch, Olaf; Dawson, Terry. *Linux Network Administrators Guide, 2nd Ed.*, June 2000, O'Reilly and Associates.

Mann, Scott; Mitchell, Ellen. *Linux System Security*, 2000, Prentice Hall PTR.

McGilton, Henry, and Rachel Morgan, 1983. *Introducing the UNIX System.* New York: McGraw-Hill Book Company.

Peterson, Richard. *Red Hat Linux: The Complete Reference*, 2000, Osborne/MacGraw-Hill.

Siever, Ellen. *Linux in a Nutshell, 2nd Ed.*, February 1999, O'Reilly and Associates.

Woolley, George, Project Manager, et al. 1990. *UNIX Made Easy.* Berkeley, CA Osborne McGraw-Hill.

General Information Sites

http://www.auscert.org.au	Australian Computer Emergency Response Team They maintain security "how to" documents.
http://www.cert.mil	Defense Information Systems Agency (DISA) JTF-GNO (Joint Task Force – Global Network Operations)
http://www.cert.org	A focal point for the computer security concerns of Internet users
http://www.ciac.llnl.gov/	The U.S. Department of Energy's Computer Incident Advisory Capability
http://www.cs.purdue.edu	COAST (Computer Operations, Audit, and Security Technology) focuses on real-world research needs.
http://www.csrc.nist.gov	National Institute of Standards and Technology's Computer Security Resource Clearinghouse
http://www.datahouse.disa.mil	Defense Information Systems Agency (DISA) Home Page
http://www.nsi.org	National Security Institute's Security Resource Net Home Page
http://www.psionic.com	Psionic Software, Inc.
http://www.redbooks.ibm.com/redbooks/homepage.html	Redbooks, named for their red covers, are "how to" books, written by very experienced IBM professionals from all over the world.
http://www.rsa.com	RSA Data Systems (encryption software)
http://www.specbench.org	The Standard Performance Evaluation Corporation
http://www.utexas.edu/cc/unix	University of Texas UNIX Services
https://vms.disa.mil	Vulnerability Management System (VMS)

APPENDIX B. HOME DIRECTORY SECURITY-RELATED FILES

NAME	***DESCRIPTION***
.cshrc	C shell initialization commands. Run at each csh invocation.
.elm	Hidden mail file
.emacs	Startup file for Gnu emacs editor
.esmvalues	Some basic values used by ESM
.exrc	Startup commands for ex and vi editors
.forward	address that tells /usr/lib/sendmail where to forward a user's electronic mail to – prohibited.
.kshrc	Korn Shell initialization commands
.login	C shell initialization commands. Run only on logon.
.logout	C shell commands executed automatically on logout
.netscape	The netscape initialization and configuration directory
.dt	The subdirectory containing CDE related files
.dtprofile	The profile used by CDE in addition to the normal .profile
.Owdefaults	OpenWindows defaults for Solaris
.profile	Bourne shell and Korn Shell initialization commands
.rhosts	Contains the names of the users who can log on to another user's account without providing a password using rsh and rlogin
.ssh2	Contains public/private keys and host information
.TTauthority	ToolTalk security file
.Xauthority	X Window system configuration security file
.Xdefaults, .Xinit, .Xresources, .Xsession	X Windows system startup files

This page is intentionally left blank.

APPENDIX C. TCP_WRAPPERS PROCEDURES

Configure the TCP_WRAPPERS program prior to compile.

- The `Makefile` should be refrenced to ensure updates and configuration options are correctly configured.

- If using a compiler other than `cc`, define the compiler environment by placing a line similar to the following line after line one of the `Makefile`:

```
CC=gcc
```

- Define where the network services daemons (such as `in.telnetd` and `in.ftpd`, or `telnetd` and `ftpd`) are normally located. For a Solaris system it will normally be `/usr/sbin`. For a HP 10.X system it will be `/usr/lbin`. For instance:

```
REAL_DAEMON_DIR=/usr/sbin
```

- Define required object libraries for the system. If this is a Solaris system, uncomment the following line:

```
LIBS  = -lsocket –lnsl      # SysV.4 Solaris 2.x
```

- If this is an HP system, uncomment the following line:

```
LIBS  = -lsyslog -lsocket -lnsl
```

- Uncomment the following line to enable banners and other extensions:

```
STYLE  = -DPROCESS_OPTIONS       # Enable language extensions
```

- Uncomment the following to enable username lookups:

```
AUTH  = -DALWAYS_RFC931
```

- Set the UMASK to a minimum of 077.

```
UMASK  = -DDAEMON_UMASK=077
```

- The following option will disconnect systems whose IP address does not match their host name. This helps protect against host name spoofing:

```
KILL_OPT  = -DKILL_IP_OPTIONS
```

The TCP_WRAPPERS program is now ready to be compiled.

- Type `make sunos5` or `make hpux` depending on the system. When compiled, make a directory for banners and badbanners:

```
mkdir /banners;mkdir /banners/badbanners
```

- Copy the `Banners.Makefile` to `/banners` and to `/banners/badbanners`.

- Copy the DOD banners file to `/banners/prototype`.

- Change directory to `/banners` and type `make`.

- Change directory to `badbanners`.

- Create a short file called `prototype` that informs the users they are not allowed to log on to this system.

- Type `make`.

- Change directory to `/etc` and create the `hosts.allow` file using the following template:

```
ALL:  192.136.137. 198.49.192. :  banners/banners
```

A much more complicated access control list could be created. This file allows the indicated networks to access any network service available on the system.

- Create the `hosts.deny` file using the following template:

```
ALL:  ALL :  banners/banners/badbanners
```

This file will disallow access to network services to all networks and hosts not defined in `/etc/hosts.allow` file.

APPENDIX D. ACKNOWLEDGEMENT OF RISK LETTER TEMPLATE

Unencrypted File Transfer
Unencrypted Terminal Sessions
30 August 2004
Version 1.1

We, the undersigned, acting as the Office of Primary Responsibility for [system/application name] and local Designated Approvinig Authority, have read the appropriate Operating System Security Technical Implementation Guide(s) (STIGs), which discuss the risks inherent in the use of (unencrypted file transfer or unencrypted terminal sessions) to perform (data transfers or terminal sessions) as part of an automated system to system interface. We have evaluated the alternatives to using (FTP or telnet) and have determined there are no currently available alternatives that meet our operational requirements. We have reviewed the risks associated with using unencrypted (file transfer or terminal sessions) and the controls that are in place to mitigate this risk. The primary risks and controls are reiterated in the following paragraphs *(the following are examples, you should detail the risk and controls below)*:

1. Maintaining automated scripts that contain userid/password pairs in a file on a system increases the potential for their compromise. As a mitigating control, we will ensure all scripts; JCL, Executive Control Language (ECL), programs, and/or data files containing one or more userid/password pairs are secured. In addition, we the office responsible for the scripts, JCL, ECL, programs, and/or data files will restrict access to the files to the fewest practical number of personnel.

2. The use of (FTP or terminal sessions) requires the userid/password and application data to be transmitted to/from the host system in clear text, across unsecured communication lines. While some data transfer can encrypt the data from point of source to destination, not all data transfer tools do. This increases the potential for compromise by various means (e.g., a sniffer program). The primary risk to the data source is disclosure of data to unauthorized persons, and the primary risk to the data destination is interception and modification of data by an unauthorized person. There is no direct mitigating control for this risk, but the office responsible for installation and configuration of the userid used for this interface will ensure the userid is configured with the lowest privilege level possible in order to limit the damage that it can do if compromised.

3. The compromise of the userid/password or application data could remain undetected for a long period of time. The password for this data transfer userid can (if justified/documented) be set to " an extended expiration," providing a procedure is developed and implemented, in coordination with the DAA and data owner, to manually change the password at least once a year or when an administrator with knowledge of the password leaves. The use of an extended expiration password increases the window of exposure to the system in the event the userid and password are compromised. This risk can be mitigated by periodic password changes even if the password is set with an extended expiration.

We will ensure the mitigating controls that must be implemented are accomplished. We will acknowledge any risks associated with not properly implementing these controls. We understand that any security violation traced back to a (FTP or telnet) may result in the suspension of system access for that userid and the security violation will be referred to the proper authorities for further investigation and action. We will ensure a copy of this letter is filed with the System Security Authorization Agreement (SSAA). This letter will be reviewed at least every 18 months or until some or all of the information below becomes outdated, or until the use of (FTP or telnet) is terminated.

Data Transfer Userid Name:	Installed on which system?
Source	Destination
Data Transfer product: (FTP, NDM, NFT, etc.)	
Data Source Information:	Data Destination Information:
System Name/ID:	System Name/ID:
Mission Assurance Category (MAC):	Mission Assurance Category (MAC):
Application Confidentiality Rating:	Application Confidentiality Rating:
Application Name:	Application Name:
File Name:	Access Level Requested:
IP Address:	IP Address:
Node Name:	Node Name:
(for NDM or other such products with Node Names)	
POC Name:	POC Name:
Alternate POC:	Alternate POC:
POC Organization:	POC Organization:
POC Phone:	POC Phone:
POC E-mail:	POC E-mail:
POC Mailing Address:	POC Mailing Address:

<signature PM for the interface data owner>	<signature local DAA>
<minimum GS-14/Military equiv>	<minimum GS-14/Military equiv.>
<typed or printed name>	<typed or printed name>
<typed or printed title>	<typed or printed title>
<typed email address>	<typed email address>
<date signed>	<date signed>

<expiration date: (18 months from date signed>

cc: <Other office involved with the interface>
<DAA for functional system>
<DISA CIO (if applicable)>

APPENDIX E. XRESOURCES AND XCONFIG FILE EXTRACTS FOR BANNERS

Locate the string `Dtlogin*greeting.labelString` in the Xresources file. Whatever is there, replace it with something similar to the following:

Dtlogin*greeting.labelString: Hello \THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM FOR WHICH MONITORING IS\nAUTHORIZED AT ALL TIMES. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED\nEQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET\nACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER\nSYSTEMS ARE SUBJECT TO MONITORING FOR ALL LAWFUL PURPOSES, INCLUDING TO\nENSURE THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO\nFACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY\nPROCEDURES, SURVIVABILITY AND OPERATIONAL SECURITY. MONITORING INCLUDES\nACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY\nOF THIS SYSTEM. DURING MONITORING, INFORMATION MAY BE EXAMINED, RECORDED,\nCOPIED AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING\nPERSONALINFORMATION, PLACED ON OR SENT OVER THIS SYSTEM IS SUBJECT TO\nMONITORING. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED,\nCONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY\nSUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED\nDURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE\nACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE\nPURPOSES.
Dtlogin*greeting.persLabelString: Hello %s\n\n\n\n\nIF YOU ARE NOT A VALID SYSTEM USER ON THIS SYSTEM GET OUT NOW!
Dtlogin*greeting.alignment: ALIGNMENT_RIGHT

Additionally, there is one change in the `Xconfig` file. Comment out the line shown and replace it with the line following it:

```
#Dtlogin*resources:      %L/Xresources
Dtlogin*resources:       Xresources
```

Then, the files must be located together in the configuration directory. For this example, the file is; `/etc/dt/config`. This, or something similar, will work on OpenWindows, Motif, etc. This particular example is for the Common Desktop Environment.

This page is intentionally left blank.

APPENDIX F. LIST OF ACRONYMS

ACL	Access Control List
AFSSI	Air Force Systems Security Instruction
AFSSM	Air Force Systems Security Memorandum
AIX	Advanced Interactive Executive
AORL	Acceptance of Risk Letter
API	Application Program Interface
AR	Army Regulation
AS	Audit Server
ASDC3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASET	Automated Security Enhancement Tool
BIND	Berkeley Internet Name Daemon
BIOS	Basic Input Output System
BSD	Berkeley Software Distribution
BSM	Basic Security Module
C3I	Command, Control, Communication, and Intelligence
CIA	Confidentiality, Integrity, and Availibility
CIFS	Common Internet Filesystem
CIS	Center of Internet Security
CMOS	Complementary Metal-Oxide Semiconductor
COAST	Computer Operations, Audit, and Security Technology
COE	Common Operating Environment
COMPUSEC	Computer Security
COOP	Continuity of Operations Plan
COPS	Computer Oracle and Password System
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
C-Time	Creation time of a file
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DES/3DES	Data Encryption Standard/Trible Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DISA WESTHEM	Defense Information Systems Agency - Western Hemisphere (formerly the Defense Information Services Organization; now the Computer Services Agency)
DLAR	Defense Logistics Agency Regulation
DLQ	Dead Letter Queue
DNS	Domain Name Service/Domain Name System
DOD	Department of Defense

DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DODIG	DOD Inspector General
EEPROM	Electrically Erasable Programmable Read-only Memory
E-mail	Electronic Mail
ESM	Enterprise Security Module
FAT	File Allocation Table
FTP	File Transfer Protocol: Defines how to transfer data from system to system.
GID	Group Identification
GOTS	Government-Off-The-Shelf
GUI	Graphical User Interface
HID	Host Based Intrusion Detection
HP-UX	Hewlett-Packard UNIX
HTTP	Hyper Text Transport Protocol
IAM	Information Assurance Manager
IAO	Information Assurance Officer
I&A	Identification and Authentication
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IM	Instant Messaging
INFOCON	Information Operations Condition
INFOSEC	Information Security
INN	Internet Network News
IP	Internet Protocol
IRC	Internet Relay Chat
ITA	Intruder Alert
JTF-GNO	Joint Task Force – Global Network Operations
KDE	K Desktop and Environment
LAN	Local Area Network
LILO	Linux Loader
MCA	Message Channel Agent
MD5	A commonly used message digest hashing algorithm
MQID	Message Queue Identification
M-Time	Modification time of a file
MVS	Multiple Virtual Storage

NAVSO	Navy Staff Office
NetBIOS	Network Basic Input/Output System
NFS	Network Filesystem
NIAP	National Information Assurance Partnership
NID	Network Intrusion Detection
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NIS	Network Information Service
NIS+	Network Information Service Plus
NNTP	Network News Transfer Protocol
NSA	National Security Agency
NSO	Network Security Officer
NSTISSP	National Security Telecommunications and Information Systems Security Policy
NTFS	New Technology Filesystem
OAM	Object Authority Manager
OASD	Office of the Assistant Secretary of Defense
OS	Operating System
OSPF	Open Shortest Path First
PC	Personal Computer
PCF	Programmable Command Format
PDF	Product Description File
P2P	Peer-to-Peer
RAS	Remote Access Service
RCERT	Regional CERT
rcp	Berkeley UNIX: remote copy program
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RPM	Red Hat Package Manager
RSA	Rivest, Shamir, and Adleman
SA	System Administrator
SAM	Security Administration Manager
SAMI	Sournce and Methods Intelligence
SATAN	Security Administrator Tool for Analyzing Networks
SCO	Santa Cruz Operation
SECNAVINST	Secretary of the Navy Instruction
SGI	Silicon Graphics Inc.
SGID	Set Group ID
SIPRNet	Secret Internet Protocol Router Network
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure

SPARC	Scalable Processor Architecture
SRR	Security Readiness Review
SSH	Secure Shell
SSL	Secure Sockets Layer
SSAA	System Security Authorization Agreement
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
SUID	Set User ID
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UID	User Identification
UUCP	UNIX to UNIX copy program
VMS	Vulnerability Management System
WESTHEM	Western Hemisphere
WWW	World Wide Web
XDM	X Display Manager