ITEM	Y	N	N/A
1. ACCOUNT ADMINISTRATION			
▪ All users have strong, non-obvious passwords)			
▪ Every user has a unique account			
▪ No users have the same user ID			
▪ Every default account's password has been changed			
▪ All guest accounts are disabled			
▪ No shared accounts exist			
▪ Format and contents of /etc/password file are appropriate and contain only authorized accounts			
▪ All accounts that have not been used for 60 or more days are disabled			
▪ No system accounts that belong to system or application developers exist on production systems			
▪ All login IDs are required and are assigned the appropriate access permissions			
▪ Privileged login IDs are strictly limited to those with specific need			
▪ Information fields in /etc/password are used to specify the precise individual or process that uses the account, including contact information			
▪ No users have a UID of 0			
▪ Every administrator has a unique user account			
▪ System does not allow user to re-choose passwords after they have expired			
▪ Users are required to change passwords every 90 days			
▪ All non-essential accounts are disabled (e.g. news)			
▪ Each account is assigned a unique password and is changed on initial login			
▪ No user accounts have a GID of 0 or 1			
▪ All accounts are disabled correctly; NOTE: This can be accomplished replacing the password with "*" and changing the login shell to /bin/false or other non-interactive program.			
▪ Separate root passwords are assigned to different machines			
2. SYSTEM ADMINISTRATION			
▪ root account is not used for activities that can be accomplished using a regular user ID			
▪ Ability to use the 'su' command to obtain root access is limited to authorized administrators			
▪ Administrators log in with individual user accounts and use 'su' to obtain root access			
▪ Backups are created regularly (daily incremental, weekly full)			

ITEM	Y	N	N/A
▪ Backups are stored securely and in a safe environment (dry, cool, fire protected etc…)			
▪ Access to backups is limited to authorized individuals			
▪ All commands have appropriate permissions set			
▪ All files that are either world or group writable are verified ▪ Use the following command to search for all files beginning with a period in the /u filesystem that are either group ro world writable: ▪ # find /u –perm –2 –o –perm –20 –name .* -ls			
▪ '.' is not in any user's (especially root) search path (users do not execute programs from the current directory)			
▪ An administrator's PATH should not begin or end with a colon (:) and there should not be two colons in sequence.			
▪ Users do not have any directory listed in their search path that is not owned by root, other system accounts, or themselves.			
▪ Initialization files for user and system accounts (e.g. start-up files, .forward files) have not been modified			
▪ No files run from cron can be modified by unauthorized users (verify permissions of all cron jobs)			
▪ All cron jobs running are authorized and applicable (cron jobs can be verified in /var/spool/cron/crontabs)			
▪ All multi-user systems have at least two designated system administrators			
▪ All user login scripts display previous login information			
▪ Only approved setuid and setgid programs exist			
▪ SUID is not set on shells, editors, or other commands that allow an escape to a shell (SUID and SGID programs usually reside in one of the following directories:/usr/etc, /usr/lib, /usr/ucb, /usr/bin, /bin, /etc, /usr/local/bin, /usr/local/etc)			
▪ Sticky bit or setuid is used for public/shared directories			
▪ The following files are renamed or do not exist:			
▪ /etc/rc2.d/S47asppp → /etc/rc2.d/K47asppp			
▪ /etc/rc2.d/S60nfs.server → /etc/rc2.d/K60nfs.server			
▪ /etc/rc2.d/S470uucp → /etc/rc2.d/K70uucp			
▪ /etc/rc2.d/S73nfs.client → /etc/rc2.d/K73nfs.client			
▪ /etc/rc2.d/S74autofs → /etc/rc2.d/K74autofs			
▪ /etc/rc2.d/S76nscd → /etc/rc2.d/K76nscd			
▪ /etc/rc2.d/S80lp → /etc/rc2.d/K80lp			
▪ /etc/rc2.d/S88sendmail → /etc/rc2.d/K88sendmail			
▪ /etc/rc2.d/S76nscd → /etc/rc2.d/K76nscd			
▪ /etc/rc3.d/S15nfs.server → /etc/rc3.d/K15nfs.server			
▪ /etc/rc3.d/S76snmpdx → /etc/rc3.d/K76snmpdx			
▪ /etc/rc3.d/S77dmi → /etc/rc3.d/K77dmi			
▪ finger services are disabled			

ITEM	Y	N	N/A
▪ Network interfaces are not running in "promiscuous" mode (verify by using the ifstatus command)			
▪ A documented disaster recovery / business continuity plan exists and has been approved by the system owner			
▪ A documented change control plan exists and has been approved by the system owner			
▪ Change control plan in 2.24 is currently being implemented			
▪ All files on system are periodically verified to ensure appropriate mode, ownership, checksums and modification dates; Records of verification process are kept off-line			
▪ root password is changed every 30 days			
▪ All duplicate commands that reside on the system are recorded, resolved and understood (ensure there are no Trojan Horses resident)			
▪ All device files reside in /dev			
3. ACCESS CONTROL			
▪ All software application passwords must be changed from their default			
▪ Every account must have a password (follow password guidelines outlined in Appendix section 7)			
▪ Passwords are not stored in plaintext anywhere on the system (e.g. text files, shell scripts, command files)			
▪ Password checkers (e.g. Crack, John the ripper) are run regularly to ensure password strength			
▪ Passwords are not communicated over e-mail			
▪ Passwords are encrypted when passed over multi-user networks			
▪ Booting to single user mode requires a password			
▪ A banner is the first message received when logging in. The banner details the system owner and describes the terms and condition of use.			
▪ Users are automatically logged out after 15 minutes of in-activity			
▪ A maximum of ten failed login attempts is allowed before locking out the session for 60 minutes			
▪ Login sessions are terminated immediately when dial-in connections are broken.			
▪ root login is restricted to the console (users should only login as root in emergencies). This is done by enabling the CONSOLE line in /etc/default/login.			
▪ FTP use is not permitted to root (add root to /etc/ftpusers)			
▪ Untrusted programs are not run as root			
▪ No write access is granted to 'other' for any terminal device file once it has been assigned to a user			
▪ All access for 'other' is denied to disk partition device files,			

ITEM	Y	N	N/A
/dev/kmem, /dev/mem			
▪ Access to the at and cron (crontab) commands are restricted to system administrators			
▪ The default umask for all users is 027			
▪ Permissions for system programs are set to the following:			
▪ Administrative executable binaries – 700			
▪ Public exectuble binaries – 751			
▪ Public shell scripts – 755			
▪ Administrative shell scripts – 700			
▪ Permissions for the following devices are set to:			
▪ Disk devices – 640			
▪ Tap devices – 660			
▪ All other devices – 600			
▪ Tty and pseudo-tty devices – 622 (and owned by root)			
▪ /dev/null devices – 777			
▪ HOME directories have permissions of 710			
▪ /var/adm/utmp has permissions of 644			
▪ Each user's .profile, .kshrc, .cshrc, .login, and other initialization files have permissions of 600			
▪ The DNS database files and /etc/named file deny all access			
▪ /etc/hosts.equiv and /etc/hosts.lpd have permissions 644			
▪ All .rhosts and .netrc files have permissions 600			
▪ /.rhosts file (if it exists) has permissions 600			
▪ /etc/inetd.conf has permissions 600			
▪ /etc/aliases has permissions 644			
▪ Only authorized users have membership in privileged groups (verify groups such as: daemon, bin, tty, staff, adm, sys, mail, uucp, rje, operator)			
▪ Login passwords are not used as encryption keys			
▪ Membership in *wheel* group (other other administrative groups) is strictly limited to authorized accounts			
▪ Password file shadowing is enabled			
▪ su logs are reviewed regularly for unauthorized login attempts. Repeated violations are investigated.			
▪ No file in /etc is group writable. (chmod –R g-w /etc)			
4. LOGGING AND AUDITING			
▪ In addition to syslog, login information is logged in the 'loginlog' file. ▪ touch /var/adm/loginlog ▪ chmod 600 /var/adm/loginlog			

ITEM	Y	N	N/A
▪ chgrp sys /var/adm/loginlog			
▪ /var/adm/messages and /var/adm/sulog are scanned regularly for bad su attempts			
▪ lastlog files are saved to track logins			
▪ Log files are backed up daily (before they are overwritten)			
▪ All logins and logouts are recorded is syslog			
▪ Access to logs is limited to authorized system administrators (e.g. su log set to 600)			
▪ Logs containing security information must be kept for a minimum of one year (off-line)			
5. OPERATING SYSTEM PATCHES AND INSTALLED SOFTWARE			
▪ All the latest ILLC approved operating system patches are installed. (use showrev –p to list the patches currently installed on the system.) The latest patches can be obtained from http://sunsolve.Sun.Com/pug-cgi/patchpage.pl :			
▪ No unauthorized software is installed			
▪ Software installed on system has been obtained from trustworthy sources and verified using a checksum			
▪ Insure that all software installed is the most current version (sendmail, ftp, bind)			
▪ All commercial software has been obtained legally			
6. NETWORK SERVICES			
▪ The following services are disabled. (To disable, preceed each of the following lines in the /etc/inetd.conf file with a pound sign, #)			
▪ `name dgram udp wait root /usr/sbin/in.tnamed in.tnamed`			
▪ `shell stream tcp nowait root /usr/sbin/in.rshd in.rshd`			
▪ `login stream tcp nowait root /usr/sbin/in.rlogind in.rlogind`			
▪ `exec stream tcp nowait root /usr/sbin/in.rexecd in.rexecd`			
▪ `comsat dgram udp wait root /usr/sbin/in.comsat in.comsat`			
▪ `talk dgram udp wait root /usr/sbin/in.talkd in.talkd`			
▪ `uucp stream tcp nowait oort /usr/sbin/in.uucpd in.uucpd`			

ITEM	Y	N	N/A
▪ `finger stream tcp nowait nobody /usr/sbin/in.fingerd in.fingerd`			
▪ `time stream tcp nowait root internal`			
▪ `time dgram udp wait root internal`			
▪ `echo stream tcp nowait root internal`			
▪ `echo dgram udp wait root internal`			
▪ `discard stream tcp nowait root internal`			
▪ `discard dgram tcp nowait root internal`			
▪ `daytime stream tcp nowait root internal`			
▪ `daytime stream udp wait root internal`			
▪ `chargen stream tcp nowait root internal`			
▪ `chargen stream udp wait root internal`			
▪ `100232/10 tli rpc/udp wait root /usr/sbin/sadmindd sadmind`			
▪ `rquotad/1 tli rpc/datagram_v wait root /usr/lib/nfs/rquotad rquotad`			
▪ `rusersd/2-3 tli rpc/datagram_v, circuit_v wait root /usr/lib/netsvc/rusers/rpc.rusersd rpc.rusersd`			
▪ `sprayd/1 tli rpc/datagram_v wait root /usr/lib/netsvc/spray/rpc.sprayd rpc.sprayd`			
▪ `walld/1 tli rpc/datagram_v wait root /usr/lib/netsvc/rwall/rpc.rwalld rpc.rwalld`			
▪ `rstatd/2-4 tli rpc/datagram_v wait root /usr/lib/netsvc/rstat/rpc.rstatd rpc.rstatd`			
▪ No network configuration files contain a "+" on a line by itself			
▪ The /etc/ftpusers file contains, at a minimum, entries for root, sysdiag, sundiag, sunc, uucp, bin, operator, daemon, audit and all other non-interactive accounts (whether or not ftp is enabled on the system)			
▪ Full DNS domain names are used for any machine name listed in files such as /etc/hosts.lpd, /etc/hosts.equiv, /etc/exports, /etc/netgroup			
▪ The /etc/hosts.equiv file is not empty (if it exists)			
▪ telnet is disabled if it is not required			

ITEM	Y	N	N/A
▪ FTP is disabled if it is not required			
▪ All r-commands are disabled (remove /etc/hosts.equiv and /.rhosts and all "r" commands from /etc/inetd.conf; execute kill –HUP on the inetd process			
▪ No users names exist in the hosts.equiv file (if it exists)			
▪ All host names (primary and aliases) on the network are unique			
▪ TFTP is disabled (If TFTP cannot be disabled permanently, it should be enabled on when needed and disabled all other times)			
▪ Anonymous FTP is disabled			
▪ UUCP is not enabled if not needed			
▪ NFS is disabled if not needed ▪ rm /etc/dfs/dfstab ▪ mv /etc/rc3.d/S15nfs.server /etc/rc3.d/K15nfs.server (removes server daemon) OR ▪ mv /etc/rc2.d/S73nfs.client /etc/rc3.d/K73nfs.client (removes client daemon)			
▪ NFS server specifies specific host names or netgroups allowed to mount file systems			
▪ NFS server permits only root access to local management server			
▪ Each user in the NFS domain has the same, unique UID on all hosts			
▪ All file systems are exported as read only			
▪ All file systems except /usr are mounted to ignore SUID permissions			
▪ All routing functions are disabled (touch /etc/notrouter)			
▪ /etc/aliases does not contain 'decode' or 'uudecode'			
▪ NIS tables do not include root or other system accounts			
▪ All mail to system accounts is sent to administrators			
▪ Mailer will not deliver a file or execute a command contained in an address line			
▪ No IRC servers are installed			
▪ No MUDs are installed			
▪ fsirand is run regularly on all exported NFS partitions			