

Windows NT 4.0 Security Checklist



1. INTRODUCTION.....	1
1.1. WORKSTATION AND SERVER.....	1
1.2. ACL DEVIATIONS.....	1
2. ADMINISTRATOR/ISSO INTERVIEW QUESTIONS.	2
2.1. PERSONNEL DATA:.....	2
2.2. USER ACCOUNTS AND SYSTEM POLICIES.....	2
2.3. EMERGENCY REPAIR DISK (ERD).....	5
2.4. FTP SERVER CONFIGURATION.....	6
2.5. DOMAIN CONTROLLER.....	6
2.6. DOCUMENTATION AND ADMINISTRATIVE TOOLS.....	7
3. System Hardware/Firmware:.....	8
3.1. CMOS SETUP.....	8
4. Operating system configuration.....	9
4.1. BOOT UP CONFIGURATION.....	9
5. SYSTEM POLICIES.....	10
5.1. LOGON CONFIGURATION.....	10
5.2. FIXED DRIVE FORMAT.....	11
5.3. ACCOUNT AND PASSWORD POLICIES.....	12
5.4. USER AND GROUP RIGHTS.....	13
6. AUDITING.....	15
6.1. USER ACCOUNT AUDIT.....	15
6.2. FILE AND DIRECTORY AUDITING.....	15
6.3. REGISTRY KEY AUDITING.....	16
6.4. LOG PROTECTION.....	17
6.5. LOG SETTINGS.....	18
7. File system configuration (ACL).....	19
7.1. FILE AND DIRECTORY ACL SETTINGS.....	19
7.2. OTHER FILES SYSTEMS AND SERVICES.....	21
8. Registry Configuration.....	22
8.1. REGISTRY PERMISSIONS.....	22
9. User configuration.....	25
9.1. ADMINISTRATORS ACCOUNTS.....	25
9.2. "GUEST" ACCOUNT.....	25
10. Removable Media.....	26
10.1. FLOPPY AND CD DRIVES.....	26

1. INTRODUCTION.

1.1. WORKSTATION AND SERVER.

1.1.1. This checklist is for the Windows NT operating system. Although the Workstation and the Server are configured nearly identically, there are a couple of differences worth noting.

1.1.1.1. As installed, NT workstation groups are Administrators, Backup Operators, Guests, Power Users, Replicator, and Users; and the NT server groups are Administrators, Backup Operators, Guests, System Operators, Replicator, and Users. The group "Power Users" is found only on the workstation and the group "System Operators" is found only on the server.

1.1.1.2. All workstations should permit "Users" to log on locally, but the server should only allow the Administrator group to log on locally.

1.1.1.3. For any servers or workstation attached to an NT domain any place where "Users" or "Administrators" are listed, "Domain Users" and "Domain Administrators" are implied.

1.2. ACL deviations.

1.2.1. The Access Control List (ACL) permissions identified in section 6 are the baseline requirements. Minor deviations from these by various organizations will occur in order to meet specific mission requirements. The ACL permissions for the Registry keys identified in section 8 may also require deviations to the HKEY_CLASSES_ROOT tree in order for some applications to operate properly.

2. ADMINISTRATOR/ISSO INTERVIEW QUESTIONS.

2.1. Personnel Data:

DMC: _____
Host Location
(bldg/room): _____
Console
Location: _____
System ID and Domain: _____
IP Address: _____
SA Name: _____
SA Phone: Comm: _____ DSN: _____
SA E-mail Address: _____
ISSO Name: _____
ISSO Phone: Comm: _____ DSN: _____
ISSO E-mail Address: _____
System Classification: _____
System Workload: _____

2.2. USER ACCOUNTS AND SYSTEM POLICIES.

2.2.1. Is physical access to Automated Information Systems controlled? Ensure by observation that the equipment and all attached ancillary devices are adequately protected. A finding exists if any hardware is not protected.

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 186.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___ NOT APPLICABLE:___

2.2.2. Are procedures in place which:

prohibit passwords from being set to words found in any dictionary or book, a users name, or their telephone number?
Require that passwords be a mix of upper and lower case letters and have at least one number or special character?

If any of these requirements are not documented and enforced, this is a finding.

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 111.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___ NOT APPLICABLE:___

2.2.3. Audit log archive and review.

Are audit logs archived?
Does the ISSO periodically review the audit logs?
Are the ISSO's reviews documented?

If the audit logs are not archived and/or the ISSO does not review the audit logs and document these reviews, this is a finding.

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 14 and 24.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___ NOT APPLICABLE:___

2.2.4. Archive protection and retention.

How are the audit logs archived and protected?

How long are archived logs retained?

If the audit logs are not downloaded to a protected media, or saved to a protected drive or partition, and retained for at least 1 year, this is a finding.

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 27.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.2.5. Does the ISSO maintain records of the existing users groups and the people that are members of them? If not, this is a finding.

X.X PDI: Standard access form DISA 41 is not being used to control system access requests.

Reference: DISA WESTHEM Security Handbook.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.2.6. Are any shared accounts in use? If shared accounts are used, this is a finding.

X.X PDI: Shared user accounts are permitted on the system.

Reference: DII COE Appendix C, Objective 286.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.2.7. Has each User with Administrative privileges been assigned a unique account with membership in the System Admin group (not the built in Admin group) to perform their Administrative tasks?

Reference: DII COE Appendix C, Objective 118 and 121.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___ NOT APPLICABLE:___

2.2.8. Do all Users with Administrative accounts have a separate account to use for operational tasks? Does anyone use the generic Administrator account? If any Administrative users are utilizing the generic Administrator account, or if they are using their individual System Admin account for normal operations, this is a finding.

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 118 and 121.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___ NOT APPLICABLE:___

2.3. EMERGENCY REPAIR DISK (ERD)

Is an ERD for each Windows NT system created at the time of system installation?
Has the ERD been updated following the last system modification?
Are all copies of the emergency repair disk protected?

If the answer to any of these is no, this is a finding.

X.X PDI: Emergency Repair Disk(s) are not created, updated, and protected according to DISA requirements.

Reference: DII COE Appendix C, Objective 163.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.4. FTP SERVER CONFIGURATION.

2.4.1. Is FTP active? (If the answer is no, proceed to section 2.5)

2.4.2. Is a separate partition on an NTFS file system the only partition to which read or write access is allowed via the FTP server; and is the FTP server configured to disallow anonymous connections?

X.X PDI: The file transfer protocol (ftp) configuration does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 132 and 134.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.5. DOMAIN CONTROLLER.

2.5.1. Where several workstations are in use, is there a primary and back up domain controller on the Domain? The Primary Domain Controller (PDC) and Backup Domain Controller (BDC) holding the SAM database can be more stringently controlled than user workstations.

X.X PDI: A Domain has not been established with both a PDC and BDC.

Reference: DII COE Appendix C, Objective 147.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.6. Documentation and Administrative Tools.

2.6.1. Are the following readily available to the Systems Administrator?

Windows NT Workstation (and Server where applicable) systems documentation.
Windows NT resource kit(s).
The utility applications DumpReg and DumpACL, or Axent Omniguard.

X.X PDI: The Systems Administrator does not have the required documentation and applications.

Reference: DII COE Appendix C, Objective 188.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

2.6.2. Is an approved Virus scan application installed and used? If an up to date, approved Virus scan program is not installed and utilized, this is a finding.

X.X PDI: An Approved Virus scan program is not used.

Reference: DII COE Appendix C, Objective 188.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

3. System Hardware/Firmware:

3.1. CMOS setup

Is the CMOS password protected?
Are boot options set to prevent booting from a floppy disk?

Note: Do not take a server off line if it will impact operational requirements to verify this setting. If necessary, question the Systems Administrator and/or the ISSO to verify that the CMOS is set properly.

- 3.1.1. During the initial boot sequence press "F1" (or the required key sequence to enter system setup). You should be prompted to enter a password before the computer will enter the CMOS Setup utility. If a password is not required, this is a finding. If the BIOS supports an option defining bootable drives you should scroll down to "Boot Options" and press enter. The settings should be as follows:

First Boot Device: Hard Disk
Second Boot Device: Disabled
Third Boot Device: Disabled
Fourth Boot Device: Disabled

If the Boot options allow anything but the hard drive to boot, this is a finding. Press ESC to return to the Main Menu. Using the arrow keys, move to the "Security" menu. If the BIOS does not support an option to define bootable drives, the User Password should also be enabled and you should be prompted for a password each time the computer is booted before the operating system is loaded. If the BIOS does not support an option to define bootable drives as stated above and the User Password is not enabled, this is a finding.

X.X PDI: The System CMOS configuration does not conform to DISA

requirements.

Reference: DII COE Appendix C, Objective 184.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

4. Operating system configuration

4.1. BOOT UP CONFIGURATION

4.1.1. Is Windows NT the only operating system installed? This can be verified during initial boot up of the computer where the screen pauses to allow the user to choose the OS to run or by selecting the Start Button, Settings, Control Panel. Open the "System" control panel and click on the Startup/Shutdown tab at the top. Click on the down arrow to the right of the Startup box. Only Windows NT boot selections should be listed. If any other operating system is listed, this is a finding.

X.X PDI: Windows NT is not the only operating system installed.

Reference: DII COE Appendix C, Objective 152.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

4.1.2. Is the most current approved Service Pack installed? During initial load of the NT operating system you will see a blue screen which lists the NT Operating System version and the service pack installed. If the computer is already running go to Start button and right click the mouse. Select Open to bring up the Start Menu box. Select "Help", then "About Windows NT". The version information and currently installed Service packs will be listed. If Service Pack 3 or greater is not installed, this is a finding.

X.X PDI: The required Service Pack is not installed.

Reference: DII COE Appendix C, Objective 153.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

5. SYSTEM POLICIES

5.1. LOGON CONFIGURATION.

- 5.1.1. Is a legal notice displayed before the logon screen appears? When Control/Alt/Delete is pressed to log on, you should see a legal notice before the logon screen appears. The text should read as follows (as a minimum):

USE OF THIS OR ANY OTHER DEPARTMENT OF DEFENSE INTEREST COMPUTER SYSTEM (DODICS) CONSTITUTES YOUR CONSENT TO MONITORING BY DOD AUTHORIZED PERSONNEL FOR COMPUTER SECURITY AND SYSTEM MANAGEMENT PURPOSES. This DODICS and all related equipment are to be used for the communication, transmission, processing, manipulation, and storage of official U.S. Government or other authorized information only. Unauthorized use of this computer may subject you to criminal prosecution and penalties.

X.X PDI: The Department of Defense (DoD) login banner is not displayed prior to a login attempt.

Reference: DII COE Appendix C, Objective 6.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

- 5.1.2. Has the shutdown button been removed from the logon screen? During initial logon, ensure that the "ShutDown" button does not appear in the logon box.

X.X PDI: The system can be shut down without logging on.

Reference: DII COE Appendix C, Objective 84.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

5.1.3. Has the logon screen been configured to not display the name of the last person logged in? During initial logon, ensure that the name of the last person logged in is not displayed in the login box.

X.X PDI: The name of the last person logged on appears in the logon box.

Reference: DII COE Appendix C, Objective 266.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

5.2. Fixed drive format

5.2.1. Are all fixed drives formatted in NTFS? From the Start Button select Programs, Administrative Tools, Disk Administrator. This will list all fixed drives recognized by the system and the type of file system on each. If any fixed drives or partitions are formatted for any other file system besides NTFS, this is a finding. (If this item is a finding, so are 6.2.1, 6.5.1 and 7.1.1)

X.X PDI: File system type is not NTFS.

Reference: DII COE Appendix C, Objective 66.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

5.3. Account and Password Policies.

- 5.3.1. Is a screen saver with password protection setup for each user account? Place the mouse pointer in the middle of the desktop and press the right mouse button. Select "Properties", this will bring up the Display control panel. Select the Screen Saver Tab. A screen saver should be selected, a delay of 15 minutes entered, and the password protected block should be checked. If the user account does not have a screen saver which is password protected, this is a finding.**

X.X PDI: User accounts are not set up with screen savers with password protection.

Reference: DII COE Appendix C, Objective 58.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

- 5.3.2. Are user account and password policies set up according to DISA requirements? From the Start Button select Programs, Administrative Tools, User Manager. Select "Policies", "Account" from the pull down menu. The chart should be configured as follows:**

Maximum Password age is set to 90days.
Minimum Password age is set to 1 day.
Password minimum length is set to at least 6 characters.
Password Uniqueness is set to "10".
The number of failed logins before lockout is set to 3 attempts.

The time period to reset the failed login attempt counter if no bad attempts is set to 30 minutes.

The Lockout Duration is set to forever.

"Users" are required to log on to change their passwords.

If any of these are not true, this is a finding.

X.X PDI: User passwords do not conform to DISA requirements.
Reference: DII COE Appendix C, Objective 108, 111, and 112.
DISA WESTHEM Security Handbook.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

5.4. USER AND GROUP RIGHTS

5.4.1. Are user and group rights configured according to DISA requirements? From the Start Button select Programs, Administrative Tools, User Manager. Select "Policies", "User Rights" from the pull down menu. Place an "X" in the Show Advanced User Rights block at the bottom, then scroll through each of the User Rights. They should be set according to Table 4-1 and if not, this is a finding.

Users Rights	Authorized Groups	Prohibited Groups
Access this Computer from the Network	Administrator, Systems Admin, Power Users, "Users	Everyone
Act as Part of the Operating System	None	All
Add Workstations to domain	Administrator, Systems Admin	Everyone
Backup Files and directories	Backup Operator	All Others
Bypass traverse checking	None	All
Change System time	Administrator, Systems Admin	
Create a Pagefile	Administrator, Systems Admin	

Users Rights	Authorized Groups	Prohibited Groups
Create a token Object	None	All
Create a permanent shared Object	None	All
Debug Programs	None.	All
Force shutdown from remote System	Administrator, Systems Admin	Everyone
Generate Security Audits	None	All
Increase Quotas	Administrator, Systems Admin	
Increase Scheduling Priorities	Administrator, Systems Admin	
Load and Unload device drivers	Administrator, Systems Admin	
Lock pages in memory	None	All
Log on as a Batch Job	None	All
Log on as a Service	None	All
Log on Locally	Users*	Everyone
Manage Auditing and Security logs	Administrator,	
Modify Firmware environment values	Administrator, Systems Admin	
Profile single process	Administrator, Systems Admin	
Profile system performance	Administrator, Systems Admin	
Replace a process level token	None	All
Restore files and directories	Backup Operators	
Shut down the system	Administrator, Systems Admin	Everyone, Guests
Take ownership of files and other objects	Administrator, Systems Admin	

Table 5-1

NOTES :

* *When there is no separate group to perform Backup, System Admin will be given this right.*

** *Where blocks are left blank, local operational requirements will dictate which groups are granted the right.*

X.X PDI: User and Group rights do not conform to DISA requirements..

Reference: DII COE Appendix C, Objective 64, 144, 263, and 284.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

6. AUDITING

6.1. USER ACCOUNT AUDIT.

6.1.1. Are significant user account events audited?
From the Start Button select Programs,
Administrative Tools, User Manager. Select
"Policies", "Auditing" from the pull down menu.
If the indicated blocks are not checked, this
is a finding.

Logon and Logoff	Success	Failure
File and Object Access		Failure
Use of User Rights		Failure
User and Group Management	Success	Failure
Security Policy Changes	Success	Failure
Restart, Shutdown, and System Process Tracking	Success	Failure

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 14, 15, and 197.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

6.2. FILE AND DIRECTORY AUDITING.

6.2.1. Are significant File and Directory events audited? From the Start Button select Programs, Windows NT Explorer. Highlight the critical directories and files, push the right mouse button, and select the security tab at the top. Select the Auditing button (as a minimum the NT root directory and it's sub-directories should be audited). If the indicated blocks are not checked, this is a finding.

Read		Failure
Write		Failure
Execute		Failure
Delete	Success	Failure
Change Permissions	Success	Failure
Take Ownership	Success	Failure

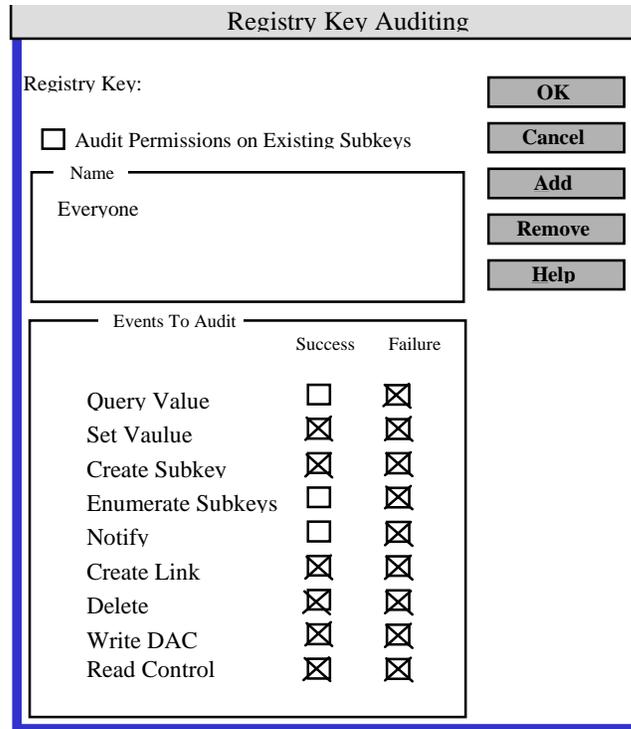
X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 14.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

6.3. REGISTRY KEY AUDITING.

6.3.1. Are the Registry Keys audited according to DISA requirements? From the Start Button select Programs, Windows NT Explorer. Go to the (NT Root Directory)\SYSTEM32 and double click on REGEDT32.EXE. This will launch the Registry editor. Select "Options" from the pull down menus and ensure that a check mark is next to "Read Only Mode" to ensure no inadvertent changes are made while inspecting the Registry Keys. Select each of the Registry Home keys (HKEY_CURRENT_USER; HKEY_CLASSES_ROOT; HKEY_USERS; and HKEY_LOCAL_MACHINE) then select "Security", and Auditing from the Pull down menu. If the Registry Key Auditing box is not configured as shown in the diagram, this is a finding.



X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 15.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

6.4. LOG PROTECTION.

6.4.1. Are the audit logs set to restrict access?

From the Start button, select Programs, Windows NT Explorer. Select the (NT root directory)\SYSTEM32\CONFIG directory. Highlight each of the following files (one at a time). right click the mouse, select Properties, then select the Security tab at the top. Select the Permission button. Each file should have the security permissions set as

indicated. If there is any deviation, this is a finding.

SysEvent.Evt	System Admin SYSTEM	Full Control Full Control
SecEvent.Evt	System Admin SYSTEM	Full Control Full Control
AppEvent.Evt	System Admin SYSTEM	Full Control Full Control

Table 6-1

X.X PDI: File and Directory permissions do not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 25.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

6.5. LOG SETTINGS.

6.5.1. Is the audit log setting configured to not overwrite audited events? From the Start button select the Programs, Administrative Tools, Event Viewer. Select Log, Log Settings from the pull down menu. The "Audit Log Full" should be set to Do Not Overwrite Events (Clear Log Manually); and the Maximum Log Size should be no less than 2048 Kilobytes. If any other "Event Log Wrapping" box is selected or the log size is set to less than 2048 Kilobytes, this is a finding.

X.X PDI: System auditing does not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 14 and 196.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

7. File system configuration (ACL)

7.1. File and Directory ACL Settings.

7.1.1. Are ACL settings configured properly? From the Start button, select Programs, Windows NT Explorer. Highlight each of the following files (one at a time). right click the mouse, select Properties, then select the Security tab at the top. Select the Permission button. Verify the designated settings. Any deviation from the table must be locally documented based on mission requirements or this is a finding.

Directory/File	Users/Groups	Permissions
C:\	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Read Full Control
C:\temp	Administrator System Admin Creator Owner Everyone SYSTEM Users	Full Control Full Control Full Control Change Full Control Change
C:\WINNT	Administrator System Admin Creator Owner Everyone SYSTEM Users	Full Control Full Control Full Control Read Full Control Change
C:\WINNT*.exe (all executable files)	Administrator System Admin Creator Owner Everyone SYSTEM Users	Full Control Full Control Full Control Read Full Control Change
C:\WINNT*.ini (all .ini files)	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Read Full Control

Directory/File	Users/Groups	Permissions
	Users	Change
C:\WINNT\System32	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Read Full Control
C:\WINNT\System	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Read Full Control
C:\WINNT\System32\Drivers	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Read Full Control
C:\WINNT\SYSTEM32\SPOOL	Administrator System Admin Creator Owner Everyone Power Users SYSTEM	Full Control Full Control Full Control Read Change Full Control
C:\BOOT.INI (This may be a hidden file)	Administrator System Admin SYSTEM	Full Control Full Control Full Control
C:\WINNT\System32\NTBackup.exe	Administrator System Admin SYSTEM	Full Control Full Control Full Control
C:\WINNT\System32\CONFIG	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control List Full Control
C:\WINNT\Repair	Administrator System Admin	Full Control Full Control
C:\WINNT\Temporary Internet Files\Desktop.ini	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Change Full Control
C:\NTDETECT.COM	Administrator System Admin SYSTEM	Full Control Full Control Full Control
C:\NTLDR	Administrator	Full Control

Directory/File	Users/Groups	Permissions
	System Admin SYSTEM	Full Control Full Control
C:\Program Files	Administrator System Admin Creator Owner Everyone SYSTEM	Full Control Full Control Full Control Add & Read Full Control

Table 7-1

X.X PDI: File and Directory permissions do not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 67, 257, 259, 260, and 262.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

7.2. OTHER FILES SYSTEMS AND SERVICES.

7.2.1. Have the built in file system and service directories and files for DHCP, OS2, and POSIX been removed? From the Start button select Programs, Windows NT Explorer. Verify that (NT root Directory) \SYSTEM32\DHCP; (NT root Directory)\SYSTEM32\OS2; and (NT root Directory)\SYSTEM32\POSIX do not exist. If any of these directories exist, this is a finding.

X.X PDI: Windows NT is not the only operating system installed.

Reference: DII COE Appendix C, Objective 67, 268, and 269.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

8. Registry Configuration

8.1. REGISTRY PERMISSIONS.

8.1.1. Are the permissions for the Registry keys properly set? From the Start button select Programs, Windows NT Explorer. Go to C:\(NT root directory)\SYSTEM32 and double click on REGEDT32.EXE. This will launch the Registry editor. Select "Options" from the pull down menus and ensure that a check mark is next to "Read Only Mode" to ensure no inadvertent changes are made while inspecting the Registry Keys. Highlight each of the each of the following Registry keys (one at a time) and verify the permissions assigned by selecting Security, Permissions from the pull down menu.

Registry Table	Key Path	Users/Groups	Permissions
HKEY_LOCAL_MACHINE	Software\ Microsoft\ RPC\ (and all subkeys)	Administrator System Admin SYSTEM Creator/owner Everyone	Full Control Full Control Full Control Full Control Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ AeDebug	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ Compatibility	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ Drivers	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ 	Everyone	Query Value, Enumerate Subkeys, Notify, and Read

Registry Table	Key Path	Users/Groups	Permissions
	Embedding		
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ Fonts	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ FontSubstitutes	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ GRE_Initialize	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ MCI	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ MCI Extensions	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ MidiMaP	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ Port (and all subkeys)	Interactive*	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ WOW (and all subkeys)	Everyone	Query Value, Enumerate Subkeys, Notify, and Read
HKEY_LOCAL_MACHINE	Software\ Mircrosoft\ Windows NT\ SYSTEM	Administrator System Admin SYSTEM	Full Control Full Control Full Control

Registry Table	Key Path	Users/Groups	Permissions
	CurrentVersion\ Run	Creator/owner Users	Full Control Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ RunOnce	Administrator System Admin SYSTEM Creator/owner Users	Full Control Full Control Full Control Full Control Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ Uninstall	Administrator System Admin SYSTEM Creator/owner Users	Full Control Full Control Full Control Full Control Read
HKEY_LOCAL_MACHINE	Software\ Microsoft\ Windows NT\ CurrentVersion\ ProfileList	Administrator System Admin SYSTEM Creator/owner Users	Full Control Full Control Full Control Full Control Query Value, Create Subkey, Enumerate Subkeys, Notify, and Read Control
HKEY_USERS	DEFAULT\ UNICODE Program Groups\ (all subkeys)	Administrator System Admin Everyone	Full Control Full Control Read
HKEY_CLASSES_ROOT	All subkeys	Administrator System Admin Creator/owner SYSTEM Everyone	Full Control Full Control Full Control Full Control Special Access **

Table 8-1

Notes:

* This should be set to **Everyone** instead of **Interactive** if a printer is to be connected directly to the printer port (LPT1) instead of using a network (Ethernet) printer connection.

** This permission is only granted **IF** use of NetScape Navigator is required on the system otherwise the permission for “Everyone” is set to “Read”. This setting opens up the HKEY_CLASSES_ROOT registry tree to attack by virus’ and/or Trojan horses run on the system since most application registry keys are located inside of this tree. To set Special Access on this key, double click on “Everyone”. This will bring up the Special access window. Place a check mark in each of the following blocks:

X.X PDI: Registry Key permissions do not conform to DISA requirements.

Reference: DII COE Appendix C, Objective 158.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

9. User configuration

9.1. ADMINISTRATORS ACCOUNTS

9.1.1. Has the built in Administrator account been renamed? From the Start button select Programs, Administrative Tools, then select User Manager. Look for the description that says "Built-in account for administering the computer/domain". If the Administrators account has not been renamed, this is a finding.

X.X PDI: The Administrative account is not configured according to DISA requirements.

Reference: DII COE Appendix C, Objective 266.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

9.2. "GUEST" ACCOUNT.

9.2.1. Has the Guest account been disabled? From the Start button select Programs, Administrative Tools, then User Manager. Double click on the Guest account and ensure that the Account Disabled block is checked. If the Guest account is not disabled, this is a finding.

X.X PDI: The Guest account has not been disabled.

Reference: DII COE Appendix C, Objective 102, 105, and 258.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

10. Removable Media

10.1.FLOPPY AND CD DRIVES.

10.1.1. Has access to floppy drives been restricted to the currently logged on user? From the Start button select Programs, Window NT Explorer. Go to (NT root directory) \SYSTEM32 and double click on REGEDT32.EXE. This will launch the Registry editor. Select "Options" from the pull down menus and ensure that a check mark is next to "Read Only Mode" to ensure no inadvertent changes are made while inspecting the Registry Keys. Select the Registry key and verify the setting

"HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon\AllocateFloppies" is set to 1.

If this registry has not been created or it is set to zero, this is a finding.

X.X PDI: Access to removable media is not restricted to the user currently logged on.

Reference: DII COE Appendix C, Objective 60.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___

10.1.2. Has the access to CD-ROM drives been restricted to the currently logged on user? From the Start button select Programs, Window NT Explorer. Go to (NT root directory) \SYSTEM32 and double click on REGEDT32.EXE. This will launch the Registry editor. Select "Options" from the pull down menus and ensure that a check mark is next to "Read Only Mode" to ensure no inadvertent changes are made while inspecting the Registry Keys. Select the Registry key and verify this setting.

"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows-NT\ CurrentVersion\WinLogon\AllocateCDRoms" is set to 1.

If this registry has not been created or it is set to zero, this is a finding.

X.X PDI: Access to removable media is not restricted to the user currently logged on.

Reference: DII COE Appendix C, Objective 60.

FINDING:___ NOT A FINDING:___ NOT REVIEWED:___NOT APPLICABLE:___