



DRAFT
WINDOWS 2003
ADDENDUM
Version 4, Release 0

9 September 2004

Developed by DISA for the DOD

UNCLASSIFIED

This page is intentionally left blank.

TABLE OF CONTENTS

SUMMARY OF CHANGES	vii
1. INTRODUCTION	9
1.1 Background	9
1.2 Authority	9
1.3 Scope	9
1.4 Writing Conventions	10
1.5 Vulnerability Severity Code Definitions	10
1.6 STIG Distribution	10
1.7 Document Revisions	11
2. SECURITY ADMINISTRATION	13
2.1 Security Controls	13
2.1.1 Open Source Software	14
2.2 Patch Control	15
2.2.1 DOD Patch Repository	15
2.2.2 Microsoft Software Updates Services (SUS)	15
2.3 Administrative Tools	16
3. SECURING THE WINDOWS 2003 OPERATING SYSTEM	17
3.1 Permitted Operating Systems	17
4. SECURING THE REGISTRY AND SERVER 2003 POLICIES	19
4.1 Windows Server 2003 Registry Access Policy	19
4.2 Windows 2003 Active Directory/Group Policy Access Policy	19
4.2.1 Group Policy Permissions	19
4.2.2 Group Policy Object Auditing	21
4.3 Registry Settings	22
4.3.1 Disable the Option to Save the Password in Dial-up Networking	22
4.3.2 Group Policy Background Refresh	22
4.3.3 Change Regedit Association	23
4.3.4 Altered DCOM RunAs Value	24
4.3.5 Restrict NetBIOS Information through SNMP	24
4.4 Access Control for Specific Registry Keys	25
4.5 Recommended Settings Variations	25
4.5.1 LMCompatibilityLevel Registry Key	25
4.5.2 AutoAdminLogon Registry Key	26
4.5.3 Password Policy	26
4.5.4 Caching of Logon Credentials	28
5. ACCOUNT POLICIES AND USER RIGHTS	29
5.1 User Rights	29
5.2 Windows Server 2003 Built-in Accounts	30
5.3 Dormant Accounts	30
5.4 Administrators Group	30

6.	AUDITING.....	31
6.1	Audit Log Management.....	31
6.1.1	Evaluating Audit Trails and Log Files.....	31
6.1.2	Protecting Logs.....	31
6.2	Audit Log Requirements.....	32
6.3	Audit Failure Procedures.....	33
6.4	System Audit Settings.....	35
6.5	File Audit Settings.....	36
6.6	Registry Audit Settings.....	37
7.	GENERAL SECURITY MEASURES.....	39
7.1	Separation of duties.....	39
7.2	DOD Physical Security Requirements.....	39
7.2.1	Restricting the Boot Process.....	40
7.3	File Security.....	41
7.3.1	Mobile USB Disk Devices.....	42
7.4	Network Printers.....	42
7.5	Logging Off or Locking the Server.....	43
7.5.1	Configuring Default User Screensaver Options.....	43
7.6	Installed Services.....	44
7.6.1	Automatic Updates Service.....	44
7.6.2	Background Intelligent Transfer Service (BITS).....	45
7.6.3	FTP Service.....	45
7.6.4	NetMeeting Remote Desktop Sharing Service.....	45
7.6.5	Print Services for UNIX.....	46
7.6.6	RCMD Service.....	46
7.6.7	Remote Access Auto Connection Manager Service.....	46
7.6.8	Remote Desktop Help Session Manager.....	46
7.6.9	Remote Registry Service.....	46
7.6.10	Remote Shell Service (RSH).....	47
7.6.11	Routing and Remote Access Service.....	47
7.6.12	Server Service.....	47
7.6.13	SNMP Service.....	48
7.6.14	Simple Service Discovery Protocol (SSDP) Service.....	48
7.6.15	Task Scheduler Service.....	48
7.6.16	Telnet Servers.....	49
7.6.17	Terminal Services.....	49
7.7	Virus Protection.....	50
7.8	Plug and Play.....	50
7.9	USB Ports.....	51
7.10	Distributed Component Object Model (DCOM).....	51
7.11	IP Forwarding.....	52
7.12	Trusted Domains.....	52
7.13	Recycle Bin.....	52
7.14	Lightweight Directory Access Protocol (LDAP).....	53
7.15	Legal Notice.....	54

8.	APPLICATION SECURITY	55
8.1	Software Configuration Management Tools.....	55
8.2	Removing Unneeded Applications	55
8.3	Application Security – Microsoft Applications	56
8.3.1	Internet Explorer Policy Settings.....	56
8.3.1.1	Security Zones: Use Only Machine Settings	56
8.3.1.2	Security Zones: Do Not Allow Users to Change Policies	56
8.3.1.3	Security Zones: Do Not Allow Users to Add/Delete Sites.....	56
8.3.1.4	Make Proxy Settings Per Machine (rather than per user).....	57
8.3.1.5	Disable Automatic Install of Internet Explorer Components	57
8.3.1.6	Disable Periodic Check for Internet Explorer Software Updates	57
8.3.1.7	Disable Software Update Shell Notifications on Program Launch	57
8.3.2	Terminal Services	58
8.3.2.1	Keep-Alive Messages	58
8.3.2.2	Limit Users to One Remote Session.....	58
8.3.2.3	Limit Number of Connections	58
8.3.2.4	Do Not Allow New Client Connections	58
8.3.2.5	Do Not Use Temp Folders per Session.....	59
8.3.2.6	Do Not Delete Temp Folder upon Exit.....	59
8.3.2.7	Set Time Limit for Idle Sessions	59
8.3.2.8	Terminate Session When Time Limits are Reached.....	59
8.3.3	Windows Installer	60
8.3.3.1	Always Install with Elevated Privileges	60
8.3.3.2	Disable IE Security Prompt for Windows Installer Scripts	60
8.3.3.3	Enable User Control Over Installs.....	60
8.3.3.4	Enable User to Browse for Source While Elevated.....	60
8.3.3.5	Enable User to Use Media Source While Elevated	61
8.3.3.6	Enable User to Patch Elevated Products.....	61
8.3.3.7	Allow Admin to Install from Terminal Services Session.....	61
8.3.3.8	Cache Transforms in Secure Location on Workstation.....	61
8.3.4	Windows Messenger.....	61
8.3.4.1	Do Not Allow Windows Messenger to be Run	62
8.3.4.2	Do Not Automatically Start Windows Messenger Initially.....	62
8.3.5	Logon.....	62
8.3.6	Group Policy	62
8.3.7	Remote Assistance	62
8.3.7.1	Solicited Remote Assistance.....	63
8.3.7.2	Remote Assistance Offers.....	63
8.3.8	Windows Time Service.....	63
8.3.9	Network Connections.....	63
8.3.9.1	Internet Connection Sharing	64
8.3.9.2	Network Bridge.....	64
8.3.10	Installation of Printers Using Kernel-mode Drivers	64
8.3.11	Media Player – Automatic Downloads	64
8.4	Application Security – Other Applications.....	65
8.4.1	MQSeries	65

8.4.2	WebSphere Application Server Security	66
8.4.3	.NET Framework	67
9.	DISASTER RECOVERY	69
9.1	Uninterruptible Power Supply (UPS)	69
9.2	Domain Backups	69
9.3	Active Directory Backups	70

APPENDICES

APPENDIX A.	REQUIRED FILE AND FOLDER PERMISSIONS	71
APPENDIX B.	REQUIRED REGISTRY KEY PERMISSIONS	85
APPENDIX C.	RELATED PUBLICATIONS	93
APPENDIX D.	WINDOWS SERVER 2003 - INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE	97
APPENDIX E.	QUICK START CHECKLIST	99
APPENDIX F.	GLOSSARY OF TERMS	105

SUMMARY OF CHANGES

September 2004:

Original Document Release

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This Addendum to Microsoft's Windows Server 2003 Security Guide has been developed to enhance the confidentiality, integrity, and availability of sensitive Department of Defense (DOD) Automated Information Systems (AISs) using the Windows Server 2003 operating system (OS).

This Addendum is coordinated with the following documents here after collectively known as the Windows Server 2003 Guides:

Microsoft "Solutions for Security, Windows Server 2003 Security Guide", 2003
Microsoft "Solutions for Security, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP", 2003.

Each site network/communications infrastructure must provide secure, available, and reliable data for all customers, especially the warfighter. This Addendum is designed to supplement the security guidance provided by the Windows Server 2003 Guides with DOD-specific requirements. This Addendum will assist sites in meeting the minimum requirements, standards, controls, and options that must be in place for secure network operations.

It should be noted that FSO Support 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 MAC II Sensitive level, containing unclassified but sensitive information.

1.3 Scope

The requirements set forth in this document will assist System Administrators (SA), Information Assurance Manager (IAM), and Information Assurance Officer (IAO), in securing the Windows Server 2003 OS for each site. The document will also assist in identifying external security exposures created when the site is connected to at least one Information System (IS) outside the site's control. The site's Configuration Control Board (CCB) will approve all major revisions to site systems.

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**” implies 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 will make 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**” is considered 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*]").

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 has 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.

1.6 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/>. The Secret Internet Protocol Router Network (SIPRNet) URL is <http://iase.disa.smil.mil/>. The National Institute of Standards and Technology (NIST) site is <http://csrc.nist.gov/pcig/cig.html>. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov** address. The STIGs

are available to users that do not originate from a **.mil** or **.gov** address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@ritchie.disa.mil**.

1.7 Document Revisions

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

This page is intentionally left blank.

2. SECURITY ADMINISTRATION

This section addresses administrative security requirements that are unique to DOD organizations and are required by DOD directives. However, the concepts outlined here are recommended to any organization requiring a framework for managing security initiatives.

2.1 Security Controls

Windows Server 2003 is an operating system in which the typical OS function and networking are integrated. It provides many configurable security features to secure both the operating system and networking functions. System-level integrity consists of protecting both hardware and software resources. The IAO will ensure a Windows Server 2003 server is configured to provide compliance with the security required by *Department of Defense (DOD) Directive 8500.1, DOD Instruction 8500.2, and OMB Circular A-130*. Use the following guidelines in the acquisition and implementation of products to ensure that security-related issues are adequately addressed:

- *(1.024: CAT II) The SA, under the direction of the IAO, will be responsible for creating, checking, and maintaining a current system baseline for all servers and critical workstations. The IAO is responsible for verifying the system baseline. The IAM will be responsible for setting overall policy for system baseline creation and maintenance.*
- *(1.024: CAT II) The IAM will ensure that sites use a baseline control tool on all servers and critical systems for which the tool is available. This does not apply to special purpose systems where it would degrade the security posture of the system. Examples are firewalls and Cross Domain Solutions (CDS) secure guards that have a minimal Operating System (OS) tailored to the specific requirements of the device.*

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, undocumented 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. The SA should maintain three weeks of baseline product reports and be able to provide them upon request. The SA should ensure that all baseline backups are maintained on write-protected media. They are most often found in the system directories but could be in other locations.

- *(1.024: CAT II) The SA will ensure that Baseline reviews are done weekly on each critical system.*

A quick way to perform a baseline review is to create a text file using the dir command. To create the initial baseline file, at the command prompt, enter **dir /s c:\winnt*. * >baseline.txt** at the C: prompt. This will send the directory contents, including all files, to the file baseline.txt on the C: drive. Be sure to enter a space between *. * and the greater than sign (>). After changes have been made, run the same command, but change the filename (baseline2.txt).

To compare the two files, open the new file (baseline2.txt) in MS Word, and perform a file comparison. In MS Word 2000, this can be found on the menu under Tools-Track Changes-Compare Documents. Any file changes will be reflected.

- (1.024: CAT II) *The SA will ensure that at a minimum, the operating system *.exe, *.bat, *.com, *.cmd, and *.dll files are baselined and compared.*
- (1.025: CAT II) *The IAM will ensure the DOD servers will use host-based Intrusion Detection Systems (IDSs) on all servers.*

NOTE: Intrusion detection will be provided at the system level. In many situations, full intrusion detection at the enclave level may not be possible due to VPN or application layer encryption.

2.1.1 Open Source 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.

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/>.”

Open source software takes several forms:

1. A utility that has publicly available source code is **acceptable**.
2. A commercial product that incorporates open source software is **acceptable** because the commercial vendor provides a warranty.
3. Vendor supported open source software is **acceptable**.

4. A utility that comes compiled and has no warranty is **not acceptable**.

2.2 Patch Control

Maintaining the security of a Windows Server 2003 system requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch (**hotfix**) to overcome security vulnerabilities.

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

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment

- *(1.029: CAT II) The IAO and SA will subscribe to the DOD-CERT/VCTS (Vulnerability Compliance Tracking System) bulletin mailing list.*
- *(2.019: CAT I) The IAO will ensure that all security-related software patches are applied and documented.*
- *(2.005: CAT II) The IAO will ensure that the latest OS and Application service packs are applied and documented.*

NOTE: Generally a couple of months will be allowed for any problems to be reported to the vendor prior to new service packs being required.

2.2.1 DOD Patch Repository

DISA maintains a repository of software patches and hot fixes.

This patch server can be accessed at the following locations:

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

SIPRNet - <https://patches.csd.disa.smil.mil>

2.2.2 Microsoft Software Updates Services (SUS)

SUS is a Microsoft's Solution for distributing and installing Windows critical updates and Windows security roll-up patches using the Autoupdate feature from a Windows client and Background Intelligent Transfer Service (BITS). This feature is only available to Windows operating systems starting with Windows 2000, SP3 and later.

Organizations that utilize SUS have options for implementation. A local SUS server can be configured to pull updates from either Microsoft or another SUS server (such as a DOD SUS server). The existence of a DOD SUS server eliminates security issues for obtaining patches,

and prevents users from downloading and applying patches that the site has not approved. Each client machine using the Software Update Services is configured to pull updates from another server running SUS. The configuration of the client allows SA's to set certain parameters for the install such as user notification that updates are available as well as the timing and notification that a reboot will occur.

The administrator of the local SUS server has configuration options that can control the deployment of each patch or allow SUS to be configured to deploy the patches as soon as they are received. This gives the flexibility to either test before deployment or have the patches immediately available for deployment.

For a client to be able to utilize an authorized SUS Server the following must be configured:

The Automatic Updates, and Background Intelligent Transfer Service (BITS) services must be active.

The following options must be configured in the Local Security Policy (or Group Policy):

Using the Local Security Policy snap-in in the MMC, expand Computer Configuration/Administrative Templates.

Right click Administrative Templates and select "Add/remove templates."

Select "Add"; then select %systemroot%\Inf\WUAU.ADM, and select "Open."

Select "Close."

Expand Administrative Templates\Windows Components\Windows Updates.

Select and enable "Configure Automatic Updates."

Select and enable "Specify intranet Microsoft update service location." Enter the appropriate web site into both server fields. ("Set the intranet update server for detecting updates" and "Set the intranet statistics server.")

Select "Close."

Exit from the MMC.

The DOD SUS server is located at the following:

NIPRNet – <http://dodsus.csd.disa.mil>

SIPRNet – <http://dodsus.csd.disa.smil.mil>

2.3 Administrative Tools

The use of automated vulnerability and intrusion detection products are recommended to assess the vulnerability of the sites' Windows Server 2003 operating systems. Microsoft has incorporated several utilities to assist in assessing Windows Server 2003 vulnerabilities.

- (1.016: CAT III) The IAO or responsible SA will use the Security Configuration Tool Set, Local Policy, or Group Policy, as described in the Windows Server 2003 Guides.

NOTE: If a manual or another configuration method is used to achieve the same result, then this will be acceptable.

3. SECURING THE WINDOWS 2003 OPERATING SYSTEM

3.1 Permitted Operating Systems

Windows Server 2003 is currently undergoing NIAP certification.

- *(5.003: CAT II) The IAO will ensure that the system boots only to STIG compliant operating systems.*
- *(2.005: CAT II) The IAO will ensure that Windows Server 2003, at a minimum, has had the latest service pack installed.*
- *(3.002: CAT II) The IAO will ensure that configuration settings and files that support the Posix operating system are removed from the machine, unless there is a documented requirement for this support.*
- *(2.020: CAT I) The IAO will ensure that unsupported system software is removed or upgraded prior to a vendor dropping support.*
- *(2.020: CAT II) The IAO will ensure that the site has a formal migration plan for removing or upgrading OS systems prior to the date the vendor drops security patch support.*

This page is intentionally left blank.

4. SECURING THE REGISTRY AND SERVER 2003 POLICIES

4.1 Windows Server 2003 Registry Access Policy

Implementing security measures within the Windows Server 2003 environment includes using the Registry Editor. Incorrect use of the Registry Editor can cause serious system-wide problems that may require the reinstallation of Windows Server 2003 to correct them. Microsoft does not guarantee that any problems resulting from the use of the Registry Editor can be solved and warns to use this tool at one's own risk. Only a highly trained SAs should modify registry settings.

- *(1.006: CAT II) The IAO will ensure that only trained, authorized SAs can access the registry to perform the Registry Editor function.*

NOTE: A system backup, to include system state data, should be created before any changes and retained for at least five working days after the changes. After changes have been completed and a successful reboot has been accomplished, an "after changes" backup should be made and maintained. If possible, a current backup that includes system state data should be available for all critical servers.

4.2 Windows 2003 Active Directory/Group Policy Access Policy

Most security measures in Windows Server 2003 are implemented using Group Policies that reside in the Active Directory. Group Policy can affect every machine in the network. Incorrect use of Group Policy could in theory bring down an entire network or cause a denial of service across an entire network. It is essential that the Active Directory and Group-level policies be protected from unauthorized or untrained persons making alterations to them.

- *(1.006: CAT II) The IAO will ensure that only trained, authorized SAs can access the Active Directory and Group-level policies for the purpose of adding policies or performing maintenance.*
- *(2.013: CAT I) The IAO will ensure that security recommendations in the Microsoft Server 2003 Guides for "Group Policy" and "Active Directory" are enforced.*

4.2.1 Group Policy Permissions

Access permissions need to be applied properly to Group Policy Objects to protect them from unauthorized access and unwanted modification. Permissions should be set for all Group Policies that may be assigned at the site, domain or organizational unit level. The procedure for setting permissions is basically the same, regardless of the level at which it is assigned.

The Group Policy is accessed through the following procedure.

Select Start -> Programs -> Administrative Tools.

Select Active Directory Users and Computers (for Domain and OU policies)

Or

Active Directory Sites and Services (for Site policies).

Select the Domain, OU or Site name in the left-hand window.

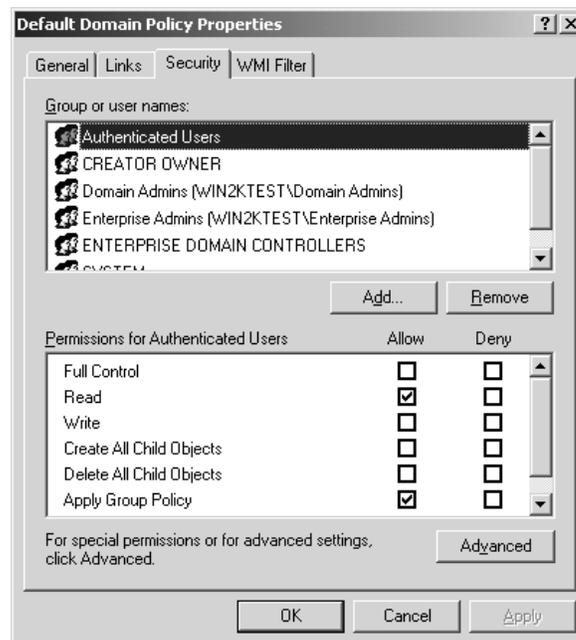
Right-click on the selected name.

Select Properties.

Select the **Group Policy** tab.

Click on **Properties**.

Select the **Security** tab.



Users should be restricted to “Read” and “Apply Group Policy.” Only *Administrator-related* groups, Creator Owner, or System can have less restrictive privileges.

The site can define more restrictive permissions by building groups that contain the specific administrators responsible for maintaining group policies and removing the more inclusive Administrator groups. Administrator responsibilities can be divided through the use of Organizational Units to more accurately reflect a division of duties. Administrators can be limited to modifying Group Policy only for the Organizational Unit for which they are responsible. This limits the scope of damage should one administrator make an accidental or malicious change that would adversely affect the network.

- (2.013: CAT I) The IAO will ensure that ACLs for Group Policies restrict access to only authorized accounts.

4.2.2 Group Policy Object Auditing

The integrity of Group Policy Objects is essential for protecting all the computers assigned to the Forest and associated Domains. Auditing should be configured on each Group Policy Object and event logs should be reviewed for failed access attempts. The default audit settings that were set at installation time should not be removed.

Group Policy audit options are accessed through the following procedure.

Select Start -> Programs -> Administrative Tools.

Select Active Directory Users and Computers (for Domain and OU policies)

Or

Active Directory Sites and Services (for Site policies).

Select the Domain, OU or Site name in the left-hand window.

Right-click on the selected name.

Select Properties.

Select the **Group Policy** tab.

Click on **Properties**.

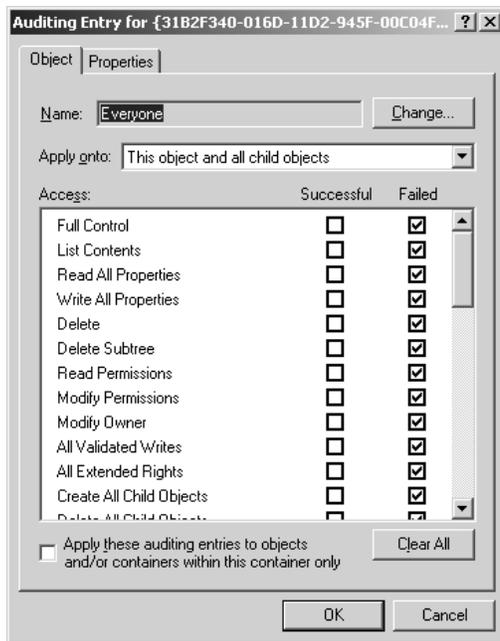
Select the **Security** tab.

Click the “**Advanced**” button and select the **Auditing** tab.

Click the “Add” button and enter “Everyone”

On the Object Tab of the Auditing Entry screen check failed option for “full control”

Click “OK”, “OK”, “OK.”



- (2.021: CAT II) The IAO will ensure that security recommendations in the Microsoft Server 2003 Guides related to Group Policy and Active Directory are enforced.

4.3 Registry Settings

The following security settings are made directly in the Registry using the **regedit.exe** editing program. On Windows 2003 machines, provision has been made to modify some of these settings through the MMC, using Security Configuration and Analysis, and Policy snap-ins. Follow the general guidance for modifying Security Options in the Windows Addendum 2003. Explicit instructions for machines, when applicable, are provided in the following sections.

The following sections outline recommended additions to the registry changes required by the *Windows Server 2003 Guide*.

NOTE: On 2003 machines, load the updated Security Options File, following instructions in the Checklist. This file adds additional CIS and FSO security configuration options to the Configuration and Analysis and Policy plug-ins.

4.3.1 Disable the Option to Save the Password in Dial-up Networking

The default Windows Server 2003 configuration enables the option to save the password used to gain access to a remote server using the dial-up networking feature. With this option enabled, an unauthorized user, who gains access, would also have access to remote servers with which the machine uses dial-up networking to communicate.

Disabling this option will introduce another layer of security and help limit the scope of any security compromise to the local machine.

- (3.024: CAT II) *The SA will ensure that the option to save a dial-up password, on machines with RAS installed, is disabled.*

The FSO modified sceregvl.inf file must be loaded for the following procedure:

Using the MMC Local Policy snap-in:

In the left-hand tree window, select Security Settings -> Local Policies -> Security Options.

In the right policy window, select the “**FSO: Prevent the dial-up password from being saved**” option and set it to **Enabled**.

NOTE: This option can also be configured using the Security Configuration and Analysis snap-in, or for multiple machines with the Group Policy snap-in.

4.3.2 Group Policy Background Refresh

This setting specifies how often domain members check to see if their group policy settings have changed. The default settings are 90 minutes with a random time of up to 30 minutes added. This default should not need to be changed. Any change should not exceed the default refresh intervals.

- (3.014: CAT III) The SA will ensure that the option to cache roaming profiles is disabled.

Using the MMC Local Policy snap-in as described in the Windows Addendum 2003:

In the left-hand tree window, select Computer Configuration -> Administrative Templates -> System -> Group Policy.

In the right policy window, select the “**Turn off background refresh of Group Policy**” option and set it to “**Disabled.**”

NOTE: This option can also be configured using the Security Configuration and Analysis snap-in, or for multiple machines with the Group Policy snap-in.

4.3.3 Change Regedit Association

If **Regedit.exe** is associated with registry files, double-clicking those files in Explorer will cause Regedit to start executing, permitting editing of the registry files. Windows Server 2003 sets up this association by default. This association should be removed. Regedit may be safely associated with an application such as Notepad.

Set the following registry key:

Hive: HKLM

Key: \Software\Classes\regfile\shell\open\command

Name: <No Name>

Type: REG_SZ

Value: notepad.exe "%1"

Select the **HKEY_LOCAL_MACHINE** on the local machine window.

Navigate down the **Software\Classes\regfile\shell\open** path, double clicking on each key along the way.

Select the **Command** key.

Edit the <**No Name**> value in the right hand window by double-clicking it.

Enter “notepad.exe "%1”” for **Value Name**:

Click **OK** in the **Add Value** window.

4.3.4 Altered DCOM RunAs Value

DCOM calls are executed under the security context of the calling user by default. If the RunAs key has been altered, the DCOM calls can be executed under the user context of the currently logged in user, or as a third user. If this ability is not carefully controlled, it could provide a network user with the ability to execute arbitrary code under another user context. RunAs values can be removed.

Set the following registry key:

Hive: HKLM

Key: \Software\Classes\AppID\

Name: "Each subkey listed"

Value: RunAs

Select the **HKEY_LOCAL_MACHINE** on the local machine window.

Navigate down the **Software\Classes\AppID** path, double clicking on each key along the way.

Select each **subkey** under the **AppID** key.

Remove any **RunAs** values found.

4.3.5 Restrict NetBIOS Information through SNMP

By default, Windows provides information that is normally available only to administrators via SNMP. Publishing information about Windows Services, users, and shares using a minimally secure protocol such as SNMP should be restricted.

Set the following registry key:

Hive: HKLM

Key: \System\CurrentControlSet\Services\SNMP\Parameters\

Name: ExtensionAgents

Value: "value containing (Software\Microsoft\LANManager\MIB2Agent\CurrentVersion)"

Select the **HKEY_LOCAL_MACHINE** on the local machine window.

Navigate down the
\System\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents path, double clicking on each key along the way.

Locate the value that contains Software/Microsoft/LANManagerMIB2Agent/CurrentVersion and remove it.

4.4 Access Control for Specific Registry Keys

Registry permissions should be configured in accordance with the guidance in *Appendix A* of this document. In addition there are other keys that require additional protection.

- (3.009: CAT II) The SA will ensure that non-administrators are not allowed to change the command associations for registry files.

Configure the following permissions:

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS
\MACHINE\Software\Classes\Regfile \Shell\Open\Command	Users Creator Owner Administrator SYSTEM	Read Read Full Control Full Control

4.5 Recommended Settings Variations

4.5.1 LMCompatibilityLevel Registry Key

Procedures for configuring the LMCompatibilityLevel Registry key for Windows Server 2003 are listed in the *Microsoft Windows 2003 Security Threats and Countermeasures guide*, pg. 85-87.

NOTE: In a mixed-mode Windows 2000 or 2003 environment, the required setting (send NTLMv2 only) for the LMCompatibilityLevel Registry key may cause authentication failures, and trust failures while trying to map shared resources in another domain. It is recommended to set the Registry key value to 1, if this problem occurs.

- (3.031: CAT II) The SA will ensure that the LMCompatibilityLevel registry key is set to the highest level that will work in your environment. At a minimum, this key must be set to at least 1. A value of 0 or no key is not acceptable.

Example:

Using the MMC Local Policy snap-in:

In the left-hand tree window, select Security Settings -> Local Policies -> Security Options.

In the right policy window, select the “LAN Manager authentication level” option and set it to “Network Security: LAN Manager authentication level.”

NOTE 1: In NT domains, set it to Send LM & NTLM – use NTLMv2 session security if negotiated. In a Windows 2000/2003 domain running **Exchange**, this setting may need to be set to not exceed level 4 “**Send NTLMv2 response/refuse LM**”, on Domain Controllers and the Exchange Server.

NOTE 2: This option can also be configured using the Security Configuration and Analysis snap-in, or for multiple machines with the Group Policy snap-in.

4.5.2 AutoAdminLogon Registry Key

This registry key can be configured to permit a machine to automatically log on as the administrator account when it is booted. This feature is used primarily to support remote installation of the operating system, and should never be enabled after the installation is completed.

Configure or delete the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon\AutoAdminLogon REG_SZ 0
```

Using the MMC Local Policy snap-in:

In the left-hand tree window, select Security Settings -> Local Policies -> Security Options.

In the right policy window, select the “FSO: Permit Administrator Automatic Logon” option and set it to “Disabled.”

Delete the following value if it exists:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows  
NT\CurrentVersion\Winlogon\DefaultPassword
```

4.5.3 Password Policy

The requirements below are exceptions and additions to the Password Policy recommended by the Microsoft Server 2003 Security Guides.

- (4.034: CAT II) *The IAM will ensure Local policy prohibits the use of weak passwords.*

- (4.011: CAT II) *The SA is ensuring maximum password age will be set to 90 days or less.*
- (4.012: CAT II) *The SA is ensuring minimum password age will be set to 1 day or more.*
- (4.002: CAT II) *The SA is ensuring Account Lockout Threshold will be set to 3 or less.*
- (4.003: CAT II) *The SA is ensuring bad logon counter reset will be set to 15 minutes or more.*
- (4.004: CAT II) *The SA is ensuring Account Lockout Duration will be set to 15 minutes or more.*
- (2.009: CAT II) *The SA is ensuring each password will be composed of at least one of each of the four character types: upper-case, lower-case, numeric, and special characters.*
- (2.009: CAT II) *The SA is ensuring the complex password filter, EnPasFlt.dll, which was developed by NSA, will be installed and active on each machine.*

NOTE 1: The use of EnPasFlt, or other external password filters, may cause a Windows 2000 Domain Controller to hang if more than 500 password change requests occur simultaneously. This problem may also exist on a Windows 2003 Domain Controller. This may occur if a utility for changing passwords is run, or an SA marks all user accounts to require a password change at the next logon, and many users log on at once. If the Domain controller should hang, the easiest solution is to reboot. The SA should try to phase password changes to limit the number being changed at once.

NOTE 2: For external password filters to be effective, the Password Policy option “Password must meet complexity requirements” must be disabled.

NOTE 3: Under Windows 2003 server, several user accounts may generate false findings in an SRR, saying that the account is not required to have a password. (i.e., Guest, IUSR_..., TSUser). The SA can correct this problem by entering the following on a command line:

Net user <account_name> /passwordreq:yes

User account Passwords must be changed at least every 90 days, and will expire after that period. However, this is not a reasonable setting for accounts that are used solely by applications. Generally, if an application account password expires, the application will cease to function. Application Accounts can be configured to not expire.

- (4.018: CAT II) *For Application accounts, the IAM will ensure that there is a local policy in place that requires passwords to be changed on a yearly basis.*

4.5.4 Caching of Logon Credentials

Windows Server 2003 will cache the credentials of users who log on interactively. In the event that a domain controller is unavailable for processing a logon, the stored credentials will permit a user to log on. This can pose a security risk if an intruder gets physical access to the machine and can get the cached credentials. To mitigate this risk the number of logon credentials stored should be limited to 1 or less.

Example:

Configure or delete the following security option:

“Interactive Logon: Number of previous logons to cache (in case Domain Controller is not available)” should be set to “0 logons” or “1 logons.”

5. ACCOUNT POLICIES AND USER RIGHTS

5.1 User Rights

The recommendations specified in the *Windows Addendum 2003* will be followed in assigning user rights. In addition, the SA will ensure that the following requirements are applied:

- (4.015: CAT I) *The SA will ensure that in Windows 2003 the built-in Guest account, Everyone group, Guests group, and Domain Guests group do not have the right to “access this computer from the network.”*
- (4.026: CAT II) *The SA will ensure the built-in Guest account, Guests group, and Domain Guests group, HelpAssistant, and Support_388945a0 are assigned to the right **deny log on locally**.*
- (4.009: CAT I) *The SA will ensure individual and group accounts do not have the right to **act as part of the operating system**.*
- (4.040: CAT I) *The SA will ensure no one has the right to allow logon through Terminal Services, unless the machine is performing the role of a Terminal Server.*
- (4.041: CAT II) *The SA will ensure the Everyone group is assigned the right deny logon through Terminal Services, unless the machine is performing the role of a Terminal Server, then the Guests group are assigned.*

NOTE: The right to **act as part of the operating system** can potentially permit an account to bypass the security features of Windows.

Therefore it is a serious security vulnerability to grant this right to any individual or group. However, some applications require this and other restricted rights to function properly. Passwords for these accounts will be the maximum length permitted, will follow the **strong password** rules, and will be kept in a locked container accessible only by the IAO and his designated backup. In this situation these restricted rights may be permitted under the following conditions:

- (4.009: CAT I) *The IAO will ensure accounts receiving this right is clearly identified and documented with the IAO in accordance with Section 2.5, Local Exceptions, of this document.*

Exceptions may be made to the recommended setting for applications that require specific rights to function properly. Vendor installation documentation will generally specify what those rights are. Generally, the rights are only required on the box on which the application is installed. Exceptions are only permissible for an application account, which is one that the application uses internally, and is never used by an individual user to log on.

- *(4.010: CAT II) The IAO will ensure that exceptions to User Rights recommendations for applications are documented.*

5.2 Windows Server 2003 Built-in Accounts

Several new accounts are created as part of the default Windows Server 2003 installation. As these accounts are well known they may represent prime attack targets. To help prevent attacks using the well-known accounts the following accounts should be disabled—HelpAssistant, Guest, and Support_388945a0.

- *(4.048: CAT II) The IAO and SA will ensure that the HelpAssistant, Guest, and Support_388945a0 accounts are disabled.*

5.3 Dormant Accounts

Accounts are considered dormant when they have not been used in 35 days. Valid accounts for individual users, who will be absent beyond this period, should be disabled to prevent their use. The intent of this requirement is for SAs to review their account listings on a regular basis and eliminate or disable accounts that are no longer active and could be used for unauthorized access.

- *(4.019: CAT III) The IAO and SA will ensure that the dormant accounts are reviewed regularly and are removed or disabled.*

NOTE: The built-in administrator account, guest account, disabled accounts, and application accounts are exempt.

5.4 Administrators Group

Members of the Administrators group have elevated privileges and permissions required for them to perform maintenance duties on the Operating System. Users who don't have Administrator duties will not be granted membership in any Administrator groups.

- *(4.027: CAT II) The IAO and SA will ensure that the regular users are not members of Administrator groups.*

6. AUDITING

6.1 Audit Log Management

6.1.1 Evaluating Audit Trails and Log Files

Auditing will be enabled and configured in accordance with the guidelines in the *Windows Server 2003 Guides* and *Section 6, Auditing*, of this document. To be of value, audit logs from servers and other critical systems will be reviewed on a daily basis to identify security breaches and potential weaknesses in the security structure.

- *(1.029: CAT II) The IAO will have local policies for archiving, reviewing, and evaluating audit trails.*

6.1.2 Protecting Logs

The Event log entries in Windows Server 2003 can be critical in providing information relating to unauthorized access to the system. To be useful as evidence in any judicial proceeding, the information in these logs must be protected and access limited to only those individuals whose job it is to evaluate and maintain these files.

File access restrictions can be set to limit the clearing and editing of the Event Logs to authorized members of an Auditors group. However, because of the structure of Windows, members of the Administrators group will still be able to view and edit the logs, if they use their privileges to modify their user rights. Therefore, local policies will preclude administrators, as a group, from changing those rights and ensure that only members of the Auditors group will be authorized change access to the Event Logs.

NOTE: The administrator(s) responsible for the installation and maintenance of the individual system(s) must be a member(s) of the Auditors group. This will permit the responsible administrator to enable and configure system auditing, and perform maintenance functions related to the logs. Administrators who are not responsible for maintenance on an individual system will not be included in the Auditors group.

- *(1.010: CAT II) The IAO or Terminal Area Security Officer (TASO), will protect Event Logs from unauthorized administrators or users who might change or delete them. All access to Event Logs will be audited, and archived logs will remain under locked control.*
- *(1.010: CAT II) The IAM will ensure Local policy precludes those accounts, which are not part of the Auditors group, from changing the file access restrictions on Windows Event Logs.*
- *(1.029: CAT II) The IAO and SA will ensure Event Logs (**APPEVENT.EVT**, **SYSEVENT.EVT**, and **SECEVENT.EVT**) are retained for at least one year. Backup and maintenance of additional log files may be required if other services are installed (i.e., IIS, SQL Server).*

- (1.029: CAT II) *The IAO will review the Event Logs on critical machines for unauthorized access daily.*
- (2.001: CAT II) *The IAO or SA will ensure Full Control access to the Event Logs is given to an Auditors group. The Auditors group contains those individuals who are authorized to archive and clear the log. (The Administrators group can be given read access.)*

NOTE: Under Windows, when an event log is cleared, the system deletes and recreates the log file. This, in effect, restores the default file permissions to those of the parent directory. Permissions for the “Auditors” group are removed and the Administrators group receives full control. To prevent the problem of having to reset permissions on the event log whenever it is cleared, use the following **optional** procedure:

Create the following directory: %SystemRoot%\system32\config\EventLogs.
Set ACL permissions on this directory. (Auditors – Full Control, System – Full Control, Administrators – Read)
Copy the event logs from the \config directory to the new EventLogs directory.
Edit the Registry using regedt32.exe.
Expand the following key: HKLM\SYSTEM\CurrentControlSet\Services\EventLog.
Select the Application key.
Double-click the “File” value.
Change the string value to: %SystemRoot%\system32\config\EventLogs\Appevent.evt.
Repeat Steps 5 through 7 for “Security (Secevent.evt)” and “System (Sysevent.evt).”
The next time the machine is rebooted it will use the event logs in the EventLogs directory.
After reboot, delete the old event logs from the \config directory.

6.2 Audit Log Requirements

Auditing is a key component in maintaining a secure computing environment. The scope of the auditing effort should be carefully planned to be consistent with operational requirements and system responsiveness. The number of machines supported may prevent a SA from implementing and managing a viable auditing effort. Every effort should be made to implement auditing according to the *Windows Server 2003 Guides* and this document.

- (4.007: CAT II) *The IAO will ensure that all are configured for auditing according to the Windows Server 2003 Guides and this document.*

Log size can be reduced if the site has an alternative auditing methodology that ensures the longevity and integrity of the data. The number of days before Event Log Wrapping occurs should be set to seven days to preserve data if a problem occurs with the alternative methodology. The Audit Server project implemented by FSO is an acceptable solution.

Microsoft recommends that the combined sizes of all event logs should not exceed 300 megabytes. On Servers this total should include any DNS and Directory Services logs. This limitation is due to the way all Windows systems handle the logs in memory. Exceeding this limit could impact system performance.

- (5.002: CAT II) The SA will ensure the maximum log size for all logs are be set to a minimum of 81920 kilobytes.
- (5.001: CAT II) The SA will ensure Event Log Wrapping is set to “ Do not overwrite Events”(Clear log manually).

6.3 Audit Failure Procedures

A site will have a documented procedure in place to identify, in a timely manner, that critical systems have stopped writing to the event logs. The procedure will include instructions for protecting and archiving log data. If a site does not have a documented procedure, then all servers and machines that a site deems critical will be configured to halt processing if an audit failure occurs.

With Windows 2000 SP3, Microsoft introduced the ability to automatically archive and clear an event log when it becomes full. This procedure works whether the setting, for halting the system if the log becomes full, is on or off. The following procedure can be used to turn on this archive function:

1. Edit the Registry using regedt32.exe.
2. Expand the following key: **HKLM\SYSTEM\CurrentControlSet\Services\EventLog**.
3. Select the appropriate event log key (e.g. Security, Application, System, etc.)
4. Select Edit -> Add Value from the Menu Bar.
5. Type “AutoBackupLogFiles” in the Value Name field, and select “REG_DWORD” in the Data Type drop-down box. Click “OK.”
6. Type a “1” in the Data field on the Dword Editor box that appears. Click “OK.”
7. Repeat Steps 3 through 6 for each event log.

The automatic archive process will create the archived log file in the %SystemRoot%\System32\Config directory. It will probably be necessary to move these files to another location on a regular basis to prevent the drive with the system files from filling up. A simple script could be written to accomplish this.

For more information on this automatic backup behavior, see Microsoft TechNet article Q312571 at <http://support.microsoft.com/default.aspx?scid=kb;en-us;312571>.

If a system has been configured to stop processing when an audit failure occurs, the system will crash with a *blue screen*, indicating that a failure event took place. At this point, only an administrator will be able to log on to the box, so that the problem can be resolved and auditing can be restarted.

The primary reason for audit failures is that the event logs have become full. Logs will need to be archived and cleared, before proceeding further with attempting to restart auditing. There are other events that can cause audit failures, but they are rare.

To reestablish auditing, follow this procedure:

- Save and clear the Event logs if necessary.
- Run Regedt32.exe and navigate to the following registry value:

Hive: HKLM

Key: \System\CurrentControlSet\Control\LSA

Name: CrashOnAuditFail

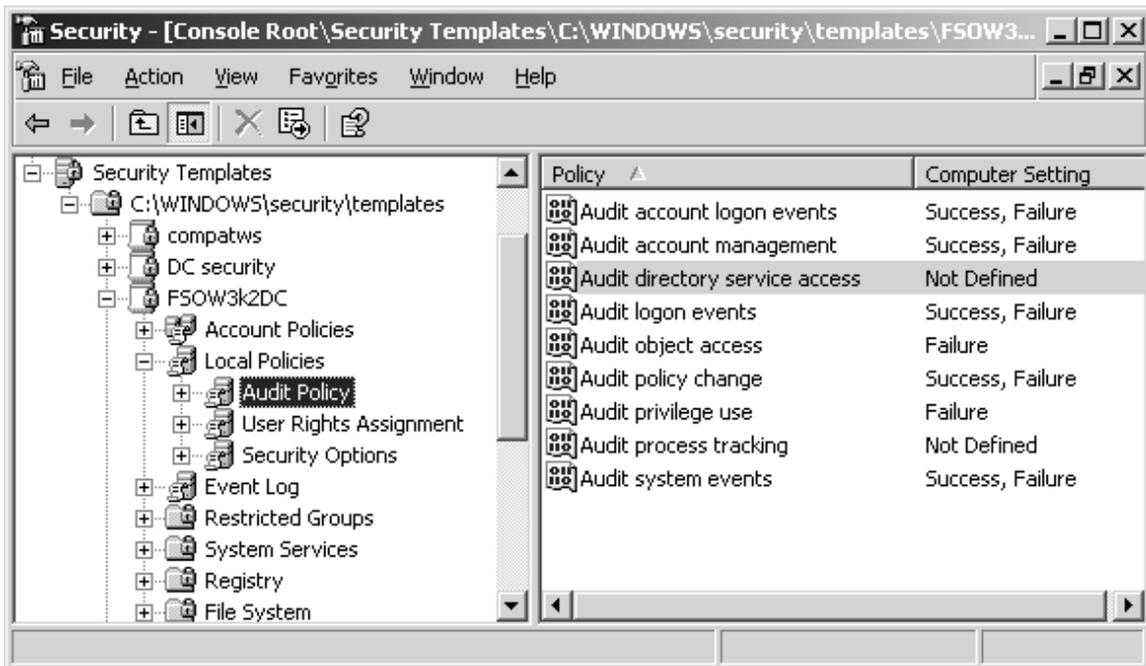
***NOTE 1:** If the CrashOnAuditFail, shows as a REG_DWORD: 0x2, change the value to a 1 and reboot the system.*

***NOTE 2:** If the CrashOnAuditFail, shows as a REG_None: 0x2, perform the following steps:*

- Highlight the CrashOnAuditFail value and press the **delete** key. Respond **yes** to the box that asks if you want to delete it.
- Highlight the LSA key, and on the menu bar, select **Edit -> Add Value**.
- Enter **CrashOnAuditFail** in the value name field, and select **REG_DWORD** in the data type box. Click **OK**.
- In the Dword editor box enter a value of **1**. Click **OK**.
- Reboot the system.

6.4 System Audit Settings

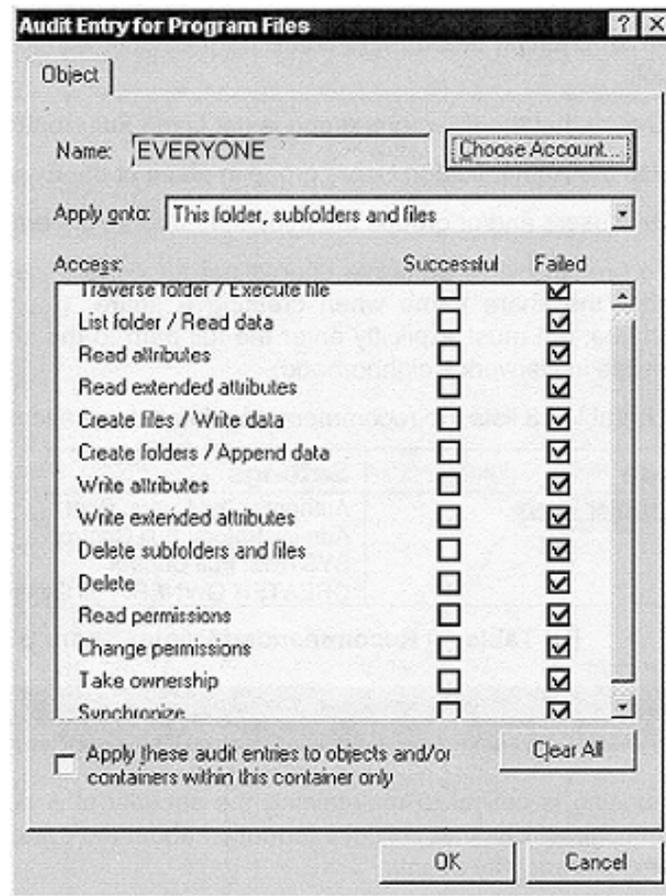
Guidance on the use and configuration of each audit setting can be found in the *Windows Server 2003 Guide*. System auditing will be configured as follows for DOD sites:



NOTE: On Domain Controllers “Audit directory service access” will be set to “Failure.”

6.5 File Audit Settings

System auditing must be configured using the procedures outlined in the *Windows Server 2003 Guide*, and section 6.4 of this document, for any file auditing settings to be effective. File auditing will be set on each local hard drive at the root directory level. The Audit Entry for the Program Files figure below displays the required settings for DOD sites.

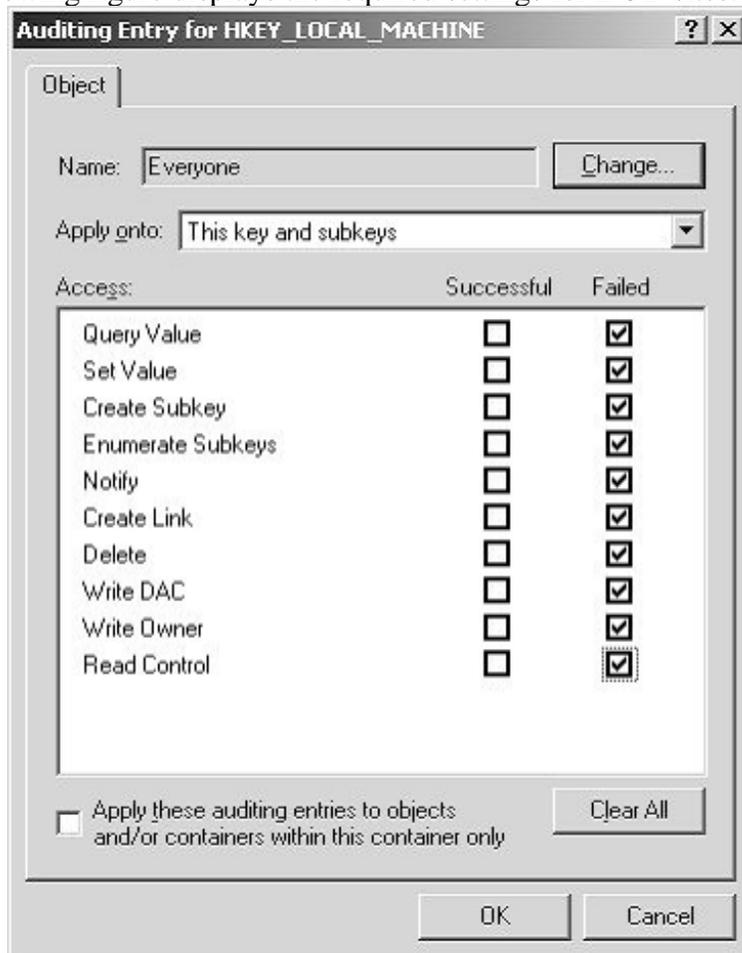


- (2.007: CAT II) The SA will ensure file auditing will be configured on each drive using the minimum requirements shown in the following figures.

6.6 Registry Audit Settings

System auditing must be configured using the procedures outlined in the *Windows Server 2003 Guide*, and section 6.4 of this document, for any registry auditing settings to be effective.

Registry auditing will be configured for the **HKEY_LOCAL_MACHINE** and **HKEY_USERS** hives. The following figure displays the required settings for DOD sites:



- (3.010: CAT II) The SA will ensure that registry auditing is configured using the minimum requirements shown in the following figures

NOTE 1: Should the site decide to audit the success Read Control this should not be done on domain controls.

NOTE 2: Audit settings are configured at the root registry key level as shown. However, after a reboot they will no longer appear here and should be checked at a subkey level (e.g. HKLM\Software), where they will be shown as being inherited.

This page is intentionally left blank.

7. GENERAL SECURITY MEASURES

7.1 Separation of duties

Personnel that have the responsibility for maintaining Operating System generally have a high level of rights and permissions on those systems. If the accounts belonging to these persons are compromised, an intruder could obtain unlimited access to critical data, or disrupt the network. To limit the risk of such exposure, personnel who have elevated access should have one privileged account for performing critical duties, and a second ordinary user account for day-to-day administrative activities (i.e. for doing email, creating documents, Internet access, etc.).

- *(1.006: CAT II) The IAO will ensure that each SA has a unique userid dedicated for administering the system.*
- *(1.006: CAT II) The IAO will ensure that each SA has a separate account for normal user tasks.*
- *(1.007: CAT II) The IAO will ensure that each Backup Operator has a unique userid dedicated for backing up the system.*
- *(1.007: CAT II) The IAO will ensure that each Backup Operator has a separate account for normal user tasks.*
- *(1.006: 1007: CAT II) The IAO will maintain a list of users belonging to Privileged groups.*
- *(1.006: 1007: CAT II) The IAO will ensure that users belonging to Privileged groups are properly trained in their duties.*

Regulations require that any activities performed on a computer system be uniquely identified with the individual user responsible. Accounts that are shared by multiple users should not be used, except in circumstances where such activities are isolated from the rest of the network (i.e. help desk, site security, etc.). Any shared account must be documented with the IAM, with justification and a risk analysis of the impact on a site's security.

- *(1.008: CAT II) The IAO will ensure that shared accounts are not used on the network.*

7.2 DOD Physical Security Requirements

No computer will ever be completely secure if people other than the authorized users can physically access it. Critical servers should be located in rooms, or locked cabinets, that are accessible only to authorized systems personnel. Physical security for Domain Controllers, Certificate servers, and especially the Schema Master is paramount for protecting the Active Directory Forest and Domains. User workstations containing sensitive data should be in access controlled areas.

- *(1.001: CAT II) The IAO will ensure that critical machines are located in access-controlled areas.*

Ensure the following for maximum security on a mission critical computer that is not physically secure (locked safely away):

- *(1.012: CAT III) Workstations will have Complimentary Metal-Oxide Semiconductor (CMOS) level password protection enabled. Each TASO will implement procedures ensuring this level of security is applied to each PC/workstation under their charge.*

NOTE: Corrupting the CMOS area will affect the entire computer, possibly making it unusable.

- *(1.012: CAT III) The IAO or TASO will ensure that the SA disables the ability to boot from removable media, if the computer hardware provides the option. (If the option does not exist, a boot password will be configured following the guidance in Section 7.2.1, Restricting the Boot Process.)*
- *(1.026: CAT III) The SA will ensure if the computer does not require network access, that the network card is removed.*

Multi-modem adapter cards that plug into Windows servers can provide a low-cost analog alternative to a dedicated remote access server. These cards fit into any Intel-based server and support up to 24 communication ports bound to Windows RAS services. Some multi-modem cards support RSA SecurID for user authentication, which can be used with a RADIUS server to provide user management, session management, and accounting services. Because server cards can be installed on domain controllers, a network administrator may inadvertently give all dial-in clients “log on locally” rights to the network. If a few permissions were to be configured improperly, a security breach could be created. Furthermore, some multi-modem cards rely solely on Windows RAS for user authentication, and do not allow for the use of the approved authentication servers.

7.2.1 Restricting the Boot Process

Setting the CMOS:

Set boot options to prevent booting from removable media. This operation will vary from computer to computer, based on the manufacturer’s specifications. During the initial boot sequence, **Press F1 to enter setup** will be displayed. (**F1** is only an example. Some systems use **F2**, **Ctrl/Del**, or **Ctrl/Esc**. Check the system’s operating manual for specific details.)

Set the computer CMOS to disallow removable media booting.

Set the Password Configuration table as follows:

Supervisor Password **ON**

User Password **OFF**

The CMOS Boot Password (Servers only):

Applies: When the option of defining which drives are bootable is not available in the system firmware, or a CMOS password cannot be set.

NOTE: This does not apply to operations systems that are shared by several SAs and are confined to a restricted, physically secure area. It does not apply to critical servers that must be continually available on a 24-hour basis.

Discussion: This makes it more difficult for intentional or unintentional booting of the computer into a non-secure operating system.

Procedures: Use procedures provided by the CMOS vendor. If necessary, upgrade the system CMOS chip.

During the initial boot sequence, press **F1** (or the required key sequence to enter system setup).

Set the Password Configuration table as follows:

Supervisor Password **ON**

User Password **ON**

Use the Supervisor password for Administrators.

7.3 File Security

File permissions will be configured to meet the recommendations in *Appendix A* of this document. Separate partitions should be created to house application files. File and directory ACLs on application partitions should be changed from the system defaults and give users only the minimum permissions required for applications to function efficiently. The Everyone group will be replaced with the Users group.

Any file share permissions should also be changed from the default, by removing the “Everyone” group and replacing it with the “Users” group, or by defining more restrictive explicit permissions.

- (2.015: CAT II) The SA will ensure that the “Everyone” group is replaced on ACLs for file shares.
- (2.015: CAT II) The SA will ensure that, on Application Servers, regular users do not have write or delete permissions to shares containing application binary files (i.e. .exe, .dll, .cmd, etc.).

7.3.1 Mobile USB Disk Devices

Mobile USB Disk devices are designed to plug into the USB port on a Windows 2000/2003/XP machine. If the Plug and Play service is running, and the USB ports are not disabled, then the device is recognized and installed without intervention, and will appear as another removable drive in Windows Explorer.

These devices are small and portable, and can be easily stolen. Physical protection of the device is essential.

These devices are also easily concealable. Generally, Windows will immediately recognize that the USB device has been connected, and will activate it. An unauthorized individual could quickly attach the device, copy sensitive files, and disconnect it in a short period of time.

If sensitive information is stored on a USB device, it should be encrypted using an encryption routine that meets DOD encryption standards. The Windows Encrypted File System or third party product can be used to encrypt files.

A user can set permissions for the files stored on the device, and also enable the system to audit any unauthorized access, by configuring the device using the Windows NTFS file system.

- *(2.017: CAT II) The IAOW will ensure that sites have a clearly defined local policy on the use of Mobile USB Disk devices.*
- *(2.017: CAT II) The IAOW will ensure that Mobile USB Disk Devices are formatted with the NTFS file system.*
- *(2.017: CAT II) The IAOW will ensure that Mobile USB Disk Devices have file ACLs and Auditing configured in accordance with DOD requirements.*

7.4 Network Printers

Printers that are shared on the network should be configured to restrict their use to authorized users. Permissions should be reconfigured to be more restrictive than the defaults assigned when the share is created. The table below shows the minimum permissions required:

Settings	
Users:	Print
Administrators:	Full Control
SYSTEM:	Full Control
CREATOR OWNER:	Full Control

- *(3.027: CAT III) The SA will ensure that print share permissions are configured according to requirements.*

7.5 Logging Off or Locking the Server

Users should either log off or lock the server if they will be away from the computer for any length of time.

Logging off allows other users to log on (if they know the password to an account); locking the session does not. If a server is not used for a set period of time, the server can be set to lock automatically by using any 32-bit screen saver with the Password Protected option.

- *(5.006: CAT II) The SA will ensure systems are configured to automatically lock with a password-protected screen saver after inactivity of no more than 15 minutes. Five minutes is recommended.*

Applications requiring continuous, real-time screen display (i.e., network management products) will be exempt from the inactivity requirement provided the following requirements are met:

The logon session does not have Administrator rights.

The inactivity exemption is justified and documented by the IAO.

The display station (i.e., keyboard, CRT) is located in a controlled access area.

7.5.1 Configuring Default User Screensaver Options

In an environment where roaming profiles are not used, every user logging on to a Windows 2003 machine for the first time has a profile built using the default user profile stored in the **%Systemdrive%\Documents and Settings** directory. The default profile can be configured to apply the password-protected screen saver requirements.

- *(3.006: CAT II) The SA will ensure the default user screensaver options will be configured to conform to DOD requirements.*

The default user profile is a registry hive, and as such, it can be edited with the following procedure:

1. Start **Regedit**. When it opens, select the **Hkey_Users** root key.
2. On the menu bar, select the **Registry>Load Hive** option to select the default user profile to be edited. It is located in the **%Systemdrive%\Documents and Settings\Default User** directory as **Ntuser.dat**.
3. When **Regedit** asks for a key name, give it a name the user recognizes. **Regedit** will import the hive and attach it under the root key under the *hive name* specified.
4. Select the new hive key, right click on it, and select **Permissions** menu item to add **Users: Read** access to the key and its subkeys. This enables the profile sharing mechanism to copy keys from the default profile to users' **Hkey_Current_Users**.

5. Use **Regedit** to make the recommended STIG changes to subkeys of the new hive. As changes are made, the hive file will be updated. Set the following values on the *hive name* \ControlPanel\Desktop key:
 - **ScreenSaveActive : REG_SZ : 1**
 - **ScreenSaverIsSecure : REG_SZ : 1**
 - **ScreenSaveTimeout : REG_SZ : 900 (in seconds, 900=15 minutes)**
 - **SCRNSAVE.EXE : REG_SZ : logon.scr**
6. Once all the hive keys are edited, use the **Registry>Unload** hive menu item to detach the hive. These settings will now be applied to a new profile when it is created.

NOTE: Use this same procedure to configure profiles that already exist on a Windows machine so that they comply with security requirements.

7.6 Installed Services

Windows Server 2003 Services typically run under two new service accounts, the Network Service and Local Service, which generally restrict permissions than are required by the service. Compromising a service could allow an intruder to obtain System permissions and open the system to a variety of attacks. The Local Service account has complete privileges on the local system. The Network Service has limited privileges on the local system.

When possible, the SA will configure services to run under local accounts with the minimum permissions and rights needed to perform their task.

- (5.068: CAT II) *The SA will remove or disable unneeded or unknown services.*
- (2.014: CAT II) *The SA will restrict access to disabled services by configuring the following ACL permissions on each service: Administrators, 'Full Control', System 'Full control', and Authenticated Users 'Read'.*
- (3.061: CAT II) *If services are to be accessed remotely (e.g., FTP), the IAO will ensure that a secure shell product is used to encrypt the userid and password.*

NOTE: Encryption of the user data inside the network firewall is also highly recommended. Encryption of user data coming from or going outside the network firewall is required. Encryption for Administrator data is always required.

7.6.1 Automatic Updates Service

This service enables the download and installation of Windows updates. As an additional security measure, if there is no requirement for its use, this service can be disabled to prevent users from downloading and installing updates that have not been approved by the site.

7.6.2 Background Intelligent Transfer Service (BITS)

This service enables the transfer of files and updates in the background using idle network bandwidth. Windows Automatic Updates and other Microsoft products use it. Downloads occur with no notification to the user until he is notified that it is present on the machine and ready to be installed. As an additional security measure, if there is no requirement for its use, this service can be disabled to prevent users from downloading and installing updates that have not been approved by the site.

7.6.3 FTP Service

The FTP Server Service allows users to access specific directories and files remotely. It is recommended that the FTP Server Service not be started on domain servers or workstations. Regular domain users should not be granted FTP access since there is already access via the shared domain directories through the Network Neighborhood icon.

If required, configure a stand-alone FTP Server with the following recommendations:

Create FTP accounts for each user
Designate one physical disk as the FTP home directory

NOTE: FTP does not encrypt passwords. If users are allowed to FTP into the domain, user account names and passwords will be transmitted in the clear. Keep in mind that anonymous users are difficult to audit.

- (5.004: CAT II) *The SA will ensure that FTP is not configured to allow prohibited logins, such as anonymous logons.*
- (5.005: CAT I) *The SA will ensure that FTP is not configured to allow access to the System drive.*

NOTE: If accounts with administrator privileges are used to access FTP, then this becomes a category I finding.

7.6.4 NetMeeting Remote Desktop Sharing Service

Microsoft has tried to make NetMeeting into a remote control utility for help desk personnel to take control of your computer in time of need. There is a risk that an exploit will be discovered, and hackers will be able to take control of vulnerable computers.

- (5.063: CAT II) *The SA will ensure that the NetMeeting Remote Desktop Sharing service is disabled.*
- (5.027: CAT II) *The IA/O and SA will ensure that the policy option for Computer -> Administrative Templates-> Windows Components -> NetMeeting **Disable remote Desktop Sharing is Enabled.***

7.6.5 Print Services for UNIX

Windows Server 2003 includes TCP/IP-based printing. You can use Print Services for UNIX to make your Windows computer work as a Line Printer Daemon (LPD) and Remote Line Printer client, manage print jobs from remote UNIX clients, and send print jobs to UNIX servers. This service is not installed by default.

- (5.026: CAT II) *If Print Services for UNIX is not required, the SA will ensure that it is removed.*

7.6.6 RCMD Service

The RCMD Service allows users to execute command line programs from remote hosts. It is distributed as part of the Windows Resource Kits. If this service is found, the **instsrv** tool that also ships with the Resource Kits can be used to remove the RCMD service.

- (5.026: CAT II) *The SA will remove the service by typing **instsrv rcmd remove** at the command prompt.*

7.6.7 Remote Access Auto Connection Manager Service

The Remote Access Auto Connection Manager Service detects unsuccessful attempts to connect to a remote network or computer and provides alternative methods for connection. With this service disabled, remote connections must be set up manually, thereby giving better control over restricting these connections.

- (5.064: CAT II) *The SA will ensure that the Remote Access Auto Connection Manager Service is disabled.*

7.6.8 Remote Desktop Help Session Manager

The Remote Desktop Help Session Manager Service manages and controls the Remote Assistance feature within the Help and Support Center application. Stopping this service will prevent remote assistance and the ability to request help.

- (5.065: CAT II) *The SA will ensure that the Remote Desktop Help Session Manager Service is disabled.*

7.6.9 Remote Registry Service

The Remote Registry Service allows you to change registry entries for a remote Windows Server 2003 computer (given the appropriate permissions). Disabling this service provides an extra level of protection to remote registries. If this service is not required, the SA should ensure that the Remote Registry Service is disabled.

7.6.10 Remote Shell Service (RSH)

A version of RSH, which ships with the Windows Resource Kits, executes all commands, regardless of user, under the **System** account. RSH is a service that allows people to configure their logon to not require a password if coming from certain machines. Intruders have figured out ways to bypass this security. The System account is the most powerful account on a Windows computer; this service will not be run under any circumstances. If this service is found, the **instsrv** tool that also ships with Resource Kits can be used to remove the RSH service.

- (5.008: CAT II) *The SA will remove the service by typing **instsrv rshsvc remove** at the command prompt.*

7.6.11 Routing and Remote Access Service

The Routing and Remote Access service is normally used either to facilitate servers as Remote Access Servers, or to allow computers from one network to interact with computers on another.

- (5.067: CAT II) *If Routing and Remote Access is not required, the SA will disable the service.*

7.6.12 Server Service

The Server Service enables systems to share resources with other systems on the network. An excellent security safeguard is to disable this service on workstations when it is not required. Several remote administration products, anti-virus products, and patch monitoring products require that this service be active.

7.6.13 SNMP Service

The SNMP Service is used to gather network management data from SNMP clients. SNMP public information may contain sensitive information that can be used to compromise a system.

- (5.026: CAT II) *If SNMP is not required, the SA will disable the service.*
- (5.057: CAT II) *The SA will ensure that SNMP communities are used to secure data.*
- (5.058: CAT II) *The SA will ensure that, if the security option “permitted managers” is enabled, a list of permitted managers is used.*
- (5.059: CAT II) *The SA will ensure that, if the security option “Traps for public community” is enabled, the list contains authorized members.*

7.6.14 Simple Service Discovery Protocol (SSDP) Service

The Simple Service Discovery Protocol (SSDP) permits discovery of UPnP devices on the network. Information can then be obtained from control points that can enable the installation of drivers for these devices. This can lead to the bypassing of a sites configuration management procedures for installing device drivers.

- (5.019: CAT I) *The SA will ensure that the SSDP Service is disabled.*

7.6.15 Task Scheduler Service

The Task Scheduler service allows administrators to schedule batch jobs to occur at specified times. Since the schedule service normally executes jobs as the System account, it can be used to modify account privileges. It is also disabled as part of the configuration needed to make a Windows machine secure. Since the schedule service requires administrator-level access to cause jobs to run, it is considered a low risk.

- (5.009: CAT II) *The SA will ensure if it is not required, the Task Scheduler service is disabled.*
- (5.009: CAT II) *The IAO will ensure that all schedule services are documented to include a list of users with access.*

In Windows 2003 additional controls can be set for Task Scheduling using the Computer Administrative Templates that are part of the system’s Local Security Policy and are also configurable through Group Policy:

The Hide Property Pages setting controls the ability to view the property pages of scheduled tasks. This will prevent users from viewing or changing the properties of a scheduled task. Administrators should be the only ones who are allowed to control a scheduled task so this setting should be enabled.

- (5.035: CAT III) *The SA will ensure that the setting Hide property page is “Enabled.”*

The Prohibit New Task Creation setting controls the ability to create new tasks using the new task wizard. Administrators are still able to schedule tasks using the **schtasks.exe** utility. Since tasks should only be scheduled by Administrators, this setting should be “Enabled.”

- (5.036: CAT III) *The SA will ensure that the setting Prohibit New Task Creation is “Enabled.”*

NOTE: In Windows Server 2003 “schtasks.exe” replaces “at.exe” as the command line task schedule utility. However, “at.exe” is still provided in the %systemroot%\system32 folder, even though it is obsolete. For security purposes, it should be deleted first from the System32\dlldata folder and then the system32 folder.

7.6.16 Telnet Servers

The Telnet service is included in the default installation of Windows 2003. In general, a Telnet server is used to access networks and applications. Telnet server products are used to let non-PC devices run character-mode DOS applications and access network-based resources.

- (5.013: CAT II) *The IAO will ensure the sites will not deploy a Windows based Telnet server.*
- (5.010: CAT II) *The SA will ensure Simple TCP/IP services will be disabled.*

7.6.17 Terminal Services

Terminal Services allow multiple users to connect from remote terminals and use the resources of the local machine as if they were physically at the machine.

- (5.020: CAT I) *The SA will ensure that Terminal Services is disabled on machines that are not performing as Terminal Servers.*

NOTE: Terminal Services may be installed in remote administration mode to support remote administration of the network within the network firewall. Remote administration from outside the firewall or through dial-up must meet encryption requirements in section 7.6.

7.7 Virus Protection

Malicious programs that result in a denial of service or corruption of data can be thwarted with scanning programs that look for signatures of known viruses. Several virus scanning and cleaning products are available for free download from the DOD-CERT group's web page. Some of the packages on the server are McAfee's AntiVirus and Symantec Norton. These are governed by a DOD site license. The address for downloading is <http://www.cert.mil> (NIPRNET) or <http://www.cert.smil.mil/antivirus/updates.htm> (SIPRNET).

The *Desktop Application STIG* provides complete requirements for anti-virus software. Configure the product using that guidance.

- (5.007: CAT I) *The SA will ensure an approved anti-virus product will be installed and enabled.*

NOTE: Some corporate firewall products, such as Raptor, are incompatible with antivirus software. On these boxes, this requirement does not apply. Personal firewall products, however, are not exempt.

- (5.007: CAT I) *The SA will ensure signature files will be no older than 14 days. (In the event that a signature file is not released by CERT in the last 14-day period, then the most current release is required).*

The use of products by DOD organizations, other than those available on the DOD-CERT web site, is discouraged. DOD has special licensing agreements with both McAfee and Symantec.

Some vendors of virus protection software make beta versions of their signature files available to their customers. These have not been tested, and should not be downloaded and used.

7.8 Plug and Play

With Windows Server 2003, plug and play installation no longer runs under the user account. A user no longer has to log on for a PnP device to be loaded. PnP devices now load before the user interacts with the system, which make these devices available during the logon process. This allows any user with physical access to the system to install devices without a site's approval. To mitigate this risk, the Plug and Play feature can be turned off with the machine's BIOS settings. However, the preferred method is to move the "driver.cab" file found in the %SystemRoot%\Driver Cache\i386 directory to a network share or to another local folder that has permissions set to limit access to Administrators. This will ensure that only Administrators can install drivers.

- (2.018: CAT III) *The SA will ensure that the "%SystemRoot%\Driver Cache\i386\driver.cab" file is moved to another folder that is restricted to Administrators.*

7.9 USB Ports

Windows Server 2003 supports the use of USB ports. If the Plug and Play service is active, a device connected to a USB port will generally be recognized and become active without user action. This feature is a vulnerability if not properly controlled. An unauthorized individual with physical access could use this feature to attach devices to a machine and obtain sensitive data.

- *(1.031: CAT II) The SA will ensure USB ports will be disabled, if they are not being used.*

7.10 Distributed Component Object Model (DCOM)

Microsoft's distributed COM (DCOM) extends the Component Object Model (COM) to support communication among objects on different computers—on a LAN, a WAN, or even the Internet. With DCOM, an application can be distributed at locations that make the most sense to the user and to the application.

DCOM achieves security transparency by letting developers and administrators configure the security settings for each component. Just as the NTFS lets administrators set access control lists (ACLs) for files and directories, DCOM stores Access Control Lists for components. These lists simply indicate which users or groups of users have the right to access a component of a certain class. These lists can easily be configured using the DCOM configuration tool (DCOMCNFG) or programmatically using the Windows 2003 registry and Win32® security functions.

- *(VI339: CAT II) The SA will ensure the default DCOM authentication level will be set at **connect** or above.*
- *(VI338: CAT II) The SA will ensure access permissions on DCOM objects will not permit non-administrators to create DCOM objects and execute code on the local system.*
- *(VI349: CAT II) The SA will ensure launch permissions on DCOM objects will not permit non-administrators to launch applications.*
- *(VI347: CAT II) The SA will ensure registry keys for DCOM objects will be configured with access permissions that prevent non-administrators from changing security settings.*

DCOMCNFG.EXE is in the **%systemroot%\System32** directory. It can be used to set access security on DCOM objects and specify the authorization level. (Select Component Services -> Computer -> My Computer. Right-click My Computer and select “properties.”)

7.11 IP Forwarding

IP Forwarding is a feature of Windows Server 2003 that in effect permits a dual-homed (multiple network cards) machine to act as a router by receiving network traffic on one network card and forwarding it through another network card. If this machine is outside of the firewall, then it could allow access to internal networks.

- *(N/A: CAT II) The SA will ensure that if IP forwarding is not allowed by the site's security policy, it is disabled.*

7.12 Trusted Domains

Trusts are used by Windows NT/2000/2003 to share resources across domains. If any of the trusted machines are compromised, the host may also be compromised. Trusts should be reviewed regularly to determine if they are required. Outdated trusts should be removed.

7.13 Recycle Bin

The Recycle Bin saves a copy of a file when it is deleted through Windows Explorer. This poses a security risk. A user may delete a sensitive file and yet still leave a copy of that file in the Recycle Bin.

- *(3.051: CAT III) The SA will ensure the Recycle Bin on servers will be configured to "remove files immediately when deleted."*

To configure the Recycle Bin to prevent deleted files from being saved, use the following procedure:

Right click the **Recycle Bin** icon on the desktop, and select **Properties**.

Check the box labeled "Do not move files to the Recycle Bin. Remove files immediately when deleted."

Click **OK**.

Empty the Recycle Bin of any pre-existing files.

7.14 Lightweight Directory Access Protocol (LDAP)

LDAP is the primary directory access protocol used to add, modify, and delete information stored in Active Directory, as well as to query and retrieve data from Active Directory. The Windows Server 2003 operating system supports LDAP versions 2 and 3. LDAP defines how a directory client can access a directory server and how the client can perform directory operations and share directory data. That is, Active Directory clients must use LDAP to obtain information from Active Directory or to maintain information in Active Directory.

Active Directory uses LDAP to enable interoperability with other LDAP-compatible client applications. **Given the appropriate permission**, you can use any LDAP-compatible client application to browse, query, add, modify, or delete information in Active Directory.

Windows 2003 LDAP itself is not configurable. It is dependent upon the security of other resources for protecting the data with which it interfaces. It is important to follow security recommendations for protecting Active Directory as well as securing TCP/IP, which is the transport mechanism for LDAP.

Locate the LDAP Service (2000/2003 Domain Controllers) behind a firewall that prevents public access.

Secure Communications. You can use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) communication and certificates to secure most communication between the Application servers and the Lightweight Directory Access Protocol (LDAP) servers. This approach is particularly important if the LDAP servers and/or their TCP ports are accessible from the Internet.

Active Directory Security. Follow the recommendations in the Windows Server 2003 Guide security guides to ensure that the data that LDAP interacts with is adequately protected.

7.15 Legal Notice

All DOD information systems will display the following “logon banner” before the logon request for user ID and password. The banner will always display when the user executes the ctrl+alt+del key sequence. This serves as sufficient proof that the banner is read.

- *(3.011: CAT II) The IAO and the SA will ensure a legal notice is displayed before console logon.*

The following is acceptable verbiage for the logon banner text.

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 US GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE 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.

The following is an acceptable logon banner title:

“US DEPARTMENT OF DEFENSE WARNING STATEMENT”

8. APPLICATION SECURITY

8.1 Software Configuration Management Tools

Software configuration management tools provide the SA a way to track and maintain site software on a network-wide basis from a central location. Products such as Tivoli and Microsoft's System Management Server (SMS) provide such a capability. Services provided by SMS include the following:

The capability to automatically gather an inventory of the hardware and software on the client workstations and servers

The capability to take control of remote workstations for troubleshooting

The capability to distribute and install software over the network in an automated fashion

The capability to provide basic network protocol analysis

The capability to interface other applications to the SMS database and develop more sophisticated applications to meet special needs

Support for an application metering package that ensures that no more copies of server-based software are run than the number of available licenses supports

- *(N/A: CAT III) The IAO will ensure that an approved software configuration management tool is used to manage the network in an automated and efficient manner.*
- *(N/A: CAT II) The IAO will ensure that only an authorized SA has access to the configuration software.*
- *(N/A: CAT III) The IAO will ensure that access to software configuration installation disks or network installation share points is restricted.*

8.2 Removing Unneeded Applications

Applications that are no longer needed should be removed from the system. Unused applications are generally not updated, or patched, and can provide a means for unauthorized persons to exploit vulnerabilities to gain access to the system. This includes Microsoft applications that may be installed when the operating system is installed

Unwanted applications should be removed using a vendor provided uninstall function or using the Windows "Add /Remove Programs" applet. It is not sufficient to just delete desktop icons and application directories. The uninstall functions also clean up the application's registry entries.

NOTE: If unwanted applications have not been completely removed using the above procedures, they will still be considered as installed for SRR and IAVM purposes.

8.3 Application Security – Microsoft Applications

In Windows Server 2003 additional controls can be set for Microsoft Applications using the Computer Administrative Templates and User Administrative Templates that are part of the system's Local Security Policy and are also configurable through Group Policy.

8.3.1 Internet Explorer Policy Settings

Internet Explorer, Microsoft's Web Browser, has been integrated with the Operating System to such an extent that it is essentially impossible to remove it from Windows. Although the option to remove the desktop and start menu icons is available, the underlying program is still there. Since it is impossible to remove, it should be configured as described in the *Desktop Application STIG* and the following settings should also be configured. In addition all patches relating to Internet Explorer must be applied to the system.

8.3.1.1 Security Zones: Use Only Machine Settings

This setting enforces consistent security zone settings to all users of the computer. Security Zones control browser behavior at various web sites and it is desirable to maintain a consistent policy for all users of a machine.

- (5.028: CAT II) *The IAO will ensure that the setting Security Zones: Use only machine settings is set to "Enabled."*

8.3.1.2 Security Zones: Do Not Allow Users to Change Policies

This setting prevents users from changing the Internet Explorer policies on the machine. Policy changes should be made by Administrators only, so this setting should be "Enabled."

- (5.029: CAT II) *The IAO will ensure that the setting Security Zones: Do not allow users to change policies is set to "Enabled."*

8.3.1.3 Security Zones: Do Not Allow Users to Add/Delete Sites

This setting prevents users from adding sites to various security zones. Users should not be able to add sites to different zones, as this could allow them to bypass security controls of the system.

- (5.030: CAT II) *The IAO will ensure that the setting Security Zones: Do not allow users to add/delete sites are set to "Enabled."*

8.3.1.4 Make Proxy Settings Per Machine (rather than per user)

This setting controls whether or not the Internet Explorer proxy settings are configured on a per-user or per-machine basis. All users of a machine should use the same proxy server to ensure consistent security policy enforcement.

- *(5.031: CAT II) The IAO will ensure that the setting Make proxy settings per-machine (rather than per user) is set to “Enabled.”*

8.3.1.5 Disable Automatic Install of Internet Explorer Components

This setting controls the ability of Internet Explorer to automatically install components if it goes to a site that requires components that are not currently installed. The SA should install all components on the system. If additional components are necessary, the user should inform the SA and have the SA install the components.

- *(5.032: CAT II) The IAO will ensure that the setting Disable Automatic Install of Internet Explorer components are set to “Enabled.”*

8.3.1.6 Disable Periodic Check for Internet Explorer Software Updates

This setting determines whether or not Internet Explorer will periodically check the Microsoft web sites to determine if there are updates to Internet Explorer available. The SA should manually install all updates on a system so that configuration control is maintained.

- *(5.033: CAT II) The IAO will ensure that the setting Disable Periodic Check for Internet Explorer software updates is set to Enabled.*

8.3.1.7 Disable Software Update Shell Notifications on Program Launch

Microsoft Internet Explorer now supports a software distribution channel that may be used to update software installed on a machine. If this setting is enabled, users will not be notified when programs are modified through the software distribution channel. A user should always be notified when a software package is updated so that unauthorized or suspicious updates may be reported.

- *(5.034: CAT II) The IAO will ensure that the setting Disable software update shell notifications on program launch is set to Disabled.*

8.3.2 Terminal Services

Terminal Services allow multiple users to connect from remote terminals and use the resources of the local machine as if they were physically at the machine. It is recommended that Terminal Services not be used on servers that are not performing the role of Terminal Servers.

8.3.2.1 Keep-Alive Messages

Keep-Alive messages are sent between the client and server to ensure that the connection state remains consistent with the client state. It is possible, in some situations, for a client to be physically disconnected from the network but for the session to remain open. If the client then reconnects, it could possibly create a new session but the original session could remain open. To prevent this from happening, Keep-Alive messages should be disabled.

- (5.037: CAT III) *The IAO will ensure that the setting **Keep-Alive Messages** is set to **Disabled**.*

8.3.2.2 Limit Users to One Remote Session

This setting limits users to one remote session. It is possible, if this setting is disabled, for users to establish multiple sessions.

- (5.038: CAT II) *The IAO will ensure that the setting **Limit users to one remote session** is set to **Enabled**.*

8.3.2.3 Limit Number of Connections

This setting limits the number of simultaneous connections allowed to the terminal server. By default, unlimited connections are allowed. Allowing unlimited connections allows a potential DoS attack. The number of incoming connections should be limited to one.

- (5.039: CAT II) *The IAO will ensure that the setting **Limit number of connections** is enabled and that the value of **TS maximum connections allowed** is no more than 1.*

8.3.2.4 Do Not Allow New Client Connections

This setting prevents new incoming connections, but does not disrupt existing connections. This setting would normally be used to **bleed-off** connections to the terminal server. Since we are currently not allowing the use of terminal services on professional machines, this setting should be enabled initially to prevent client connections.

- (5.040: CAT II) *The IAO will ensure that the setting **Do not allow new client connections** is set to **Enabled**.*

8.3.2.5 Do Not Use Temp Folders per Session

This setting, which is located under the **Temporary Folders** section of the Terminal Services configuration option, controls the use of per session temporary folders or of a communal temporary folder. If this setting is enabled, only one temporary folder is used for all terminal services sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

- (5.044: CAT II) The IAO will ensure that the setting **Do not use temp folders per session** is set to **Disabled**.

8.3.2.6 Do Not Delete Temp Folder upon Exit

This setting, which is located under the **Temporary Folders** section of the Terminal Services configuration option, controls the deletion of the temporary folders when the session is terminated. Temporary folders should always be deleted after a session is over to prevent hard disk clutter and potential leakage of information.

- (5.045: CAT II) The IAO will ensure that the setting **Do not delete temp folder upon exit** is set to **Disabled**.

8.3.2.7 Set Time Limit for Idle Sessions

This setting, which is located under the **Sessions** section of the Terminal Services configuration option, controls how long a session may be idle before it is automatically disconnected from the server. Users should disconnect if they plan on being away from their terminals for extended periods of time. Idle sessions should be disconnected after 15 minutes.

- (5.047: CAT II) The IAO will ensure that the setting **Set time limit for idle sessions** is set to **Enabled** and that the **Idle session limit** is set to no more than 15 minutes.

8.3.2.8 Terminate Session When Time Limits are Reached

This setting, which is located under the **Sessions** section of the Terminal Services configuration option, controls whether or not clients are forcefully disconnected if their terminal services time limit is exceeded. If time limits are established for users, they should be enforced.

- (5.049: CAT II) The IAO will ensure that the setting **Terminate session when time limits are reached** is set to **Enabled**.

8.3.3 Windows Installer

Windows Installer packages are structured packages being used for the distribution of software. Many new software products are using this distribution format, and the settings in this section control some of the installer's behavior.

8.3.3.1 Always Install with Elevated Privileges

If the Windows Installer is allowed to execute with elevated privileges, it can access areas of the system and perform actions that the account used to launch the installer may normally not launch. This could lead to unapproved software being installed or access to resources that the user cannot normally access.

- (4.037: CAT II) The IAO will ensure that the setting *Always install with elevated privileges* is set to *“Disabled.”*

8.3.3.2 Disable IE Security Prompt for Windows Installer Scripts

If this setting is enabled, users are not prompted when a web-based program attempts to install software on the system. Users should always be notified and asked for permission before a software package is installed to help prevent the installation of malicious software.

- (5.050: CAT II) The IAO will ensure that the setting *Disable IE security prompt for Windows Installer scripts* is set to *“Disabled.”*

8.3.3.3 Enable User Control Over Installs

This setting permits users to change installation settings that are normally only available to SAs. To do this, several Windows Installer security checks are bypassed. This setting should be disabled to prevent users from changing software installation options.

- (5.051: CAT II) The IAO will ensure that the setting *Enable user control over installs* is set to *“Disabled.”*

8.3.3.4 Enable User to Browse for Source While Elevated

This setting controls the ability of the user to browse the disk if an installer package executing with elevated privileges is executing. This could allow a user to access directories that they normally may not access.

- (5.052: CAT II) The IAO will ensure that the setting *Enable user to browse for source while elevated* is set to *“Disabled.”*

8.3.3.5 Enable User to Use Media Source While Elevated

This setting allows users to install programs from removable media when executing an installer package that is running with elevated privileges.

- *(5.053: CAT II) The IAO will ensure that the setting Enable user to use media source while elevated is set to “Disabled.”*

8.3.3.6 Enable User to Patch Elevated Products

This setting enables users to patch a product that was installed with elevated privileges. Such patching may result in the corruption or replacement of critical files and should not be allowed.

- *(5.054: CAT II) The IAO will ensure that the setting Enable user to patch elevated products is set to “Disabled.”*

8.3.3.7 Allow Admin to Install from Terminal Services Session

This setting allows Terminal Services Administrators to install and administer software remotely. Until Terminal Services is fully evaluated, it should not be used.

- *(5.055: CAT II) The IAO will ensure that the setting Allow admin to install from Terminal Services session is set to “Disabled.”*

8.3.3.8 Cache Transforms in Secure Location on Workstation

Transforms are control files that specify many settings in customized installations of software packages that use the Windows installer. Normally a copy of the transform file is stored in the user's profile. The transform file may contain critical system information and should be stored in a secure location on the machine, instead of in a user's profile.

- *(5.056: CAT II) The IAO will ensure that the setting Cache transforms in secure location on workstation is set to “Enabled.”*

8.3.4 Windows Messenger

Windows messenger is an instant messaging (IM) application created and distributed by Microsoft. There have been recent virus releases that use the Windows messenger client as a distribution method, since most virus scanners do not currently scan IM messages or files. In addition, IM clients require registration with a central server and may be the target of DoS or other attacks.

Windows Messenger also requires users to create a Microsoft Passport account in order to use the messenger. Passport accounts are also created if a user signs up for an e-mail account on the Hotmail e-mail service. Several security vulnerabilities have been discovered recently in the Passport system that could lead to a compromise of the information stored on the passport servers.

8.3.4.1 Do Not Allow Windows Messenger to be Run

This setting prevents the Windows Messenger client from being run. Since the client is currently vulnerable to several types of attacks, users should be prevented from launching it.

- *(5.017: CAT I) The IAO will ensure that the setting Do not allow Windows Messenger to be run is set to “Enabled.”*

8.3.4.2 Do Not Automatically Start Windows Messenger Initially

This setting prevents the automatic launch of Windows Messenger at user logon.

- *(5.029: CAT I) The IAO will ensure that the setting Do not automatically start Windows Messenger initially is set to “Enabled.”*

8.3.5 Logon

In general, it is good practice to ensure that all computer-related group policy changes are applied prior to users logging on so that the user can operate under the correct security context. Therefore, the following group policy setting is recommended:

- Navigate down to the Computer Configuration\Administrative Templates\System\Logon option
- In the right pane, double-click Always wait for the network at computer startup and logon
- Click the **Enabled** radio button
- Click **OK**

- *(3.067: CAT II) The IAO will ensure that the setting Always Wait for the Network at Computer Startup and Logon is set to “Enabled.”*

8.3.6 Group Policy

The Group Policy section contains several settings that control the refresh intervals and application rules that apply to group policy. The following setting ensures group policy settings are refreshed properly. If this setting is enabled, then Group Policy settings are not refreshed while a user is currently logged on. This could lead to instances when a user does not have the latest changes to a policy applied and is therefore operating in an insecure context.

- *(3.080: CAT II) The IAO will ensure that the setting Turn off background refresh of Group Policy is set to “Disabled.”*

8.3.7 Remote Assistance

Remote Assistance (RA) is a capability that allows a user to request assistance from another person. Using this technology the other person may view the user’s computer screen and send

them messages or, if the user's computer settings allow it, the other person has the ability to take control of the user's system and simultaneously interact directly with the desktop. This feature can allow unimpeded access to sensitive information.

RA can be initiated via a user request, known as Solicited Remote Assistance, or by an external person offering assistance to the user, known as Remote Assistance Offers.

8.3.7.1 Solicited Remote Assistance

Currently there is no way to limit who a novice can request assistance from; the invitation can be sent to virtually anyone who has physical connectivity to the user's network. This feature must be disabled.

- *(3.068: CAT I) The IAO will ensure that the setting Solicited Remote Assistance is set to "Disabled."*

8.3.7.2 Remote Assistance Offers

Remote Assistance Offers are viewed as the more secure way to provide assistance to users. Offers are only available between two machines in the same domain or trusted domains, and the list of users who are allowed to offer such assistance is configurable. When using this capability, an expert cannot connect to a user's system unannounced or control it without explicit permission from the user. The user is still given the opportunity to accept or deny the connection.

It is recommended that you never allow users the ability to give another person remote control of their computer. Although the user can watch their actions and take back control at any time, it can only take a second to compromise a machine or make it inoperable.

- *(3.082: CAT II) The IAO will ensure that the setting Offer Remote Assistance is set to "Disabled."*

8.3.8 Windows Time Service

The Windows Time Service controls time synchronization settings. Time synchronization is essential for authentication and auditing purposes. The Windows Time Service attempts to synchronize with the Microsoft time server time.windows.com. If the Windows Time Service is used, it should synchronize with a secure, authorized time source, and not the Microsoft time server.

- *(3.084: CAT II) The IAO will ensure that if the value for "Configure Windows NTP Client" is set to "Enabled", the "NtpServer" field points to an authorized time source.*

8.3.9 Network Connections

Settings under network connections control certain behavior when connected to a network

8.3.9.1 Internet Connection Sharing

Internet connection sharing allows the computer to act as a gateway for other systems to access the Internet. It uses network address translation (NAT) to provide connections to multiple computers through a single Internet connection. This should not be used on a network as it could allow unauthorized machines access to the network.

- *(3.085: CAT II) The IAO will ensure that the setting Prohibit use of Internet Connection Sharing on your DNS domain network is set to “Enabled.”*

8.3.9.2 Network Bridge

A network bridge is used to connect various network segments to each other. Network bridges should be dedicated hardware, and workstations should not be used for this purpose.

- *(3.086: CAT II) The IAO will ensure that the setting Prohibit installation and configuration of Network Bridge on your DNS domain network is set to “Enabled.”*

8.3.10 Installation of Printers Using Kernel-mode Drivers

Kernel-mode drivers are drivers that operate in **kernel mode**. Kernel mode allows virtually unlimited access to hardware and memory. A poorly written kernel driver may cause system instability and data corruption. Malicious code inserted in a kernel-mode driver has almost no limit on what it may do. Most modern printers do not require kernel-mode drivers.

- *(3.087: CAT II) The IAO will ensure that the setting Disallow installation of printers using kernel-mode drivers is set to “Enabled.”*

8.3.11 Media Player – Automatic Downloads

The Windows Media Player uses software components, referred to as CODECs, to play back media files. By default, when an unknown file type is opened with the Media Player it will search the Internet for the appropriate CODEC and automatically download it. To ensure platform consistency and to protect against new vulnerabilities associated with media types, the SA must install all CODECs.

- *(5.061: CAT II) The IAO will ensure that the setting Prevent Codec Download is set to “Enabled.”*

The automatic check for updates performed by the Windows Media Player for XP must be disabled to ensure a constant platform and to prevent the introduction of unknown/untested software on the network. Creating the following registry key will prevent the Media Player from checking for automatic updates.

- (5.060: CAT II) The IAO will ensure that the following registry key exists and that its value is set to "1":

KEY:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\WindowsMediaPlayer\DisableAutoupdate

TYPE: REG_DWORD

VALUE: 1

8.4 Application Security – Other Applications

8.4.1 MQSeries

MQSeries is a communications utility developed by International Business Machines (IBM) that runs on multiple platforms (OS/390, UNIX, NT, WIN2K, XP, W2K3, Tandem, etc.) and can use multiple protocols (TCP, UDP, and LU 6.2). It is a client/server suite, but a single system can be configured with both the client and the server software. The "series" consists of several related components. The most important feature is the ability to pass data between applications on heterogeneous systems. It accomplishes this by using message queues and channel interfaces.

MQSeries provides transaction processing between Windows, UNIX, and IBM mainframe systems. MQSeries provides a mechanism for host and channel Identification and Authentication (I&A). Other security must be provided through user-supplied "xit" programs or channel security exits. There is no built-in mechanism to provide data encryption for messages (queries). Data encryption is accomplished with user-defined message exits. MQSeries will interface with native security systems to perform security I&A and access authority validation using the various security exits.

When MQSeries runs on Windows Server 2003, it defaults to the operating system for all security. The MQSeries installation process will install the software in a directory called MQSeries and create a group account called MQM.

- (8.001: CAT II) The SA will ensure the MQSeries default local group account called MQM is used.

NOTE: A Domain account with MQM in its name can be created if needed for MQSeries applications.

- (8.002: CAT II) The SA will ensure that only user accounts allowed in either the local or domain MQM groups are those that need access to the MQSeries application.
- (8.003: CAT III) The SA will ensure the access control permissions on the MQSeries directory, sub-directories, and files is set in accordance with Appendix A of the NT and WIN2K SRR Checklists.
- (8.004: CAT II) The SA will ensure MQSeries services are configured to run under a local account, not the system account.

- (8.005: CAT II) The SA will ensure the MQSeries log is configured to preserve events and not overwrite.
- (8.006: CAT II) The SA will ensure that the Queue Manager log is configured to preserve events and not overwrite.
- (8.007: CAT III) The SA will ensure versions of the older MQ.ini and QM.ini configuration files are removed from the MQSeries\Config directory.
- (8.008: CAT I) The SA will ensure the MCAUSER attribute on MQSeries Clients contains a non-blank value or point to a security exit.

NOTE: If any server connection channel contains a blank value, then this is a finding. If a Channel Security Exit is in use, and provides a user identifier, then the MCAUSER attribute can be blank and will not be a finding.

8.4.2 WebSphere Application Server Security

WebSphere is an IBM software product used to develop, implement, and manage web sites, web applications, and web applications that have been integrated into non-web applications. WebSphere makes use of a Java development and run-time environment that allows WebSphere to execute Java programs and Web applications.

WebSphere is dependent upon the security features of the Windows Server 2003 operating system for protecting sensitive information and for authenticating users.

The following are requirements for WebSphere Application Server to function properly in the Microsoft Windows environment:

A WebSphere application account must be created and be a member of the Administrator's group.

The WebSphere application account must have the rights to "Log on as a service" and "Act as part of the operating system."

The Browser service must be active.

Several of the WebSphere configuration files contain userids and passwords. These are needed at run time to access external secure resources such as databases. Passwords are encoded, not encrypted, to deter casual observation of sensitive information. Password encoding combined **with proper operating system file system security** is intended to protect the passwords stored in these files. The key and trust store passwords in the **sas.client.props** are not encoded. The default WebSphere installation directory is \WebSphere, and the \WebSphere\Appserver directory is normally the store for sensitive property files (keyring files) containing passwords.

To properly secure WebSphere, the IAO and SA will ensure that the following steps are taken:

- (8.011: CAT II) *The SA will create a separate security userid and grant the necessary permissions to perform administrative functions, for using the WebSphere Administrative Console.*
- (8.012: CAT II) *The SA will configure WebSphere to use NT authentication in Windows NT domains. Configure it to use Active Directory for authentication in Windows 2000/2003 domains.*

WebSphere is dependent upon operating system security for protecting sensitive files and authenticating users. Permissions to WebSphere files and directories should be limited to those users and groups that need access. At a minimum, the WebSphere Application will need “Full Access.”

- (8.013: CAT II) *The SA will ensure that the following files are protected:*

Directories containing the JAVA programs, JAVA beans, JAVA servlets, and web applications used by WebSphere. Access is limited to the WebSphere account and WebSphere administrators.

Directories containing XML files, which contain security attributes for enterprise JAVA beans and web applications. These files may contain password data, as well as other sensitive information.

Directories containing the WebSphere Administrative Console functions.

The WebSphere client keyring file “sas.server.props” contains sensitive information and certificate information that is not encoded. It is located in the installation root\properties directory.

Any directories containing files used in the development or execution of code that is used by WebSphere.

8.4.3 .NET Framework

The Microsoft .NET Framework, also referred to as the Common Language Runtime (CLR), provides an operating environment similar to the Java Runtime Engine (JRE). Programs written and compiled to the .NET Platform may be run on any system with a CLR installed, regardless of the underlying OS.

One of the principal goals of the .NET Platform is to provide a common operating environment for web-based applications. .NET mobile code is currently uncategorized. According to the DOD mobile code policy, uncategorized mobile code is not allowed to execute on any DOD system. The .NET Framework may only be used for locally developed applications.

The .NET Framework includes a complex security model that is currently being evaluated. It is integrated into the Windows Server 2003 operating system. Until the security model, new programming languages, and the platform itself are evaluated, the .NET Framework will not be active on any DOD systems, except when used to support locally developed .NET applications.

- *(5.069: CAT II) The IAO will ensure that the .NET Framework is not active on the system, unless it only supports locally developed .NET applications.*

Microsoft has already released a Service Pack for the .NET Framework that fixes several problems. If the .NET Framework is installed, it must be upgraded to current .NET Framework Service Pack.

- *(5.069: CAT II) The IAO will ensure that the .NET Framework, if it is installed, is upgraded to the current Service Pack.*

9. DISASTER RECOVERY

9.1 Uninterruptible Power Supply (UPS)

An Uninterruptible Power Supply (UPS) is a key element in maintaining continuity of operations in the event of power failure or fluctuation. It will give critical machines the time needed to shut down normally and prevent loss or corruption of data.

- *The IAO or TASO will ensure that each Windows 2003 production server is on a UPS.*

The UPS product must deliver not just reliable backup power in the event of a blackout, but clean, steady power around the clock to prevent data loss and equipment failure. The UPS should be either an on-line or line-interactive UPS product. Most on-line UPSs provide what is called dual-source power to continuously condition and correct the incoming power. They take AC from the wall, convert it to DC, regulate it, and then convert it back to AC power.

9.2 Domain Backups

Backup of critical machines and data will be accomplished in accordance with the guidance in DODI 8500.2".

A system backup, to include system state data, should be created before any major changes to the operating system and retained for at least five working days after the changes. After changes have been completed and a successful reboot has been accomplished, an "after changes" backup should be made and maintained. A current backup that includes system state data should be available for all critical servers.

- *(1.013: CAT III) The IAM will ensure the site maintains emergency system recovery data for each critical system.*
- *(1.013: CAT III) The IAM will ensure the emergency system recovery data is protected from destruction and stored in locked storage container.*
- *(1.013: CAT III) The IAM will ensure the site maintains emergency system recovery data for each critical Windows 2003 system created at the time of system installation.*
- *(1.013: CAT III) The IAM will ensure the emergency system recovery data is updated following each significant system modification.*

9.3 Active Directory Backups

Active Directory is the heart of a windows Server 2003 domain. If the Active Directory becomes corrupted, and no backup copy exists, it will probably be necessary to reinstall the entire domain. Therefore, it is essential to maintain a current backup, to ensure a timely continuance of operations should problems occur. SAs should ensure that a current backup of the Active Directory is made prior to making any significant changes.

- *(1.023: CAT II) The Active Directory will be backed up on Server 2003 domain controllers on a weekly basis.*

APPENDIX A. REQUIRED FILE AND FOLDER PERMISSIONS

Folders and files not explicitly listed below are assumed to inherit the permissions of their parent folder. Folders with **Do not allow permissions on this file or folder to be replaced** are explicitly excluded from security configuration and retain their original permissions. The term “Replace” indicates that the **Replace existing permissions on all subfolders and files with inheritable permissions** radio button should be enabled while “Propagate” indicates that the **Propagate inheritable permissions to all subfolders and files** radio button should be enabled.

Unless otherwise noted, permissions are assumed to apply to all subfolders and files below the configured folder.

On Domain Controllers the Group “Users” should be replaced with “Authenticated Users.”

FOLDER OR FILE	USER GROUPS	REQUIRED PERMISSIONS	INHERIT METHOD
%SystemDrive% Folder, subfolders, and files	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users	Full Control Full Control Full Control RX	Propagate
%SystemDrive%\AUTOEXEC.BAT	Administrators Users SYSTEM	Full Control RX Full Control	Replace
%SystemDrive%\BOOT.INI	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\CONFIG.SYS	Administrators Users SYSTEM	Full Control RX Full Control	Replace
%SystemDrive%\IO.SYS	Administrators Users SYSTEM	Full Control RX Full Control	Replace
%SystemDrive%\MSDOS.SYS	Administrators Users SYSTEM	Full Control RX Full Control	Replace

FOLDER OR FILE	USER GROUPS	REQUIRED PERMISSIONS	INHERIT METHOD
%SystemDrive%\NTBOOTDD.SYS	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\NTDETECT.COM	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\NTLDR	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\ 	Administrators SYSTEM Users	Full Control Full Control R X	Propagate
%SystemDrive%\Documents and Settings\Administrator <i>(or profile of renamed account)</i>	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\All Users NOTE: If WINDOWS 2003 has been reinstalled over another copy of the operating system, additional All Users profile folders will be created in the Documents and Settings folder. Typically, the new profile is called All Users.WINDOWS or All Users.COMPUTERNAME. Prior copies of the All Users folder, although still existing, will not be used. The %AllUsersProfile% environment variable will automatically point to the profile currently in use. To determine which profile is actually being used, see the HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\AllUsersProfile registry key value.	Administrators SYSTEM Users	Full Control Full Control RX	Propagate
%SystemDrive%\Documents and Settings\All Users\Application Data	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users Users	Full Control Full Control Full Control R X Write (subfolders & files)	Propagate

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft	Administrators SYSTEM Users	Full Control Full Control R X	Replace
%SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\Crypto\DSS\MachineKeys	Administrators SYSTEM Users	Full Control Full Control List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Read permissions (this folder only)	Replace
%SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys	Administrators SYSTEM Users	Full Control Full Control List folder, Read attributes, Read extended attributes, Create files, Create folders, Write attributes, Write extended attributes, Read permissions (this folder only)	Replace
%SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\DrWatson Folder containing Dr. Watson application error log.	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users Users	Full Control Full Control Full Control R X Traverse folder, Create files, Create folders (subfolders and files)	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\All Users\Application Data\DrWatson\drwtsn32.log NOTE: This setting only has significance if the drwtsn32.log file has already been created. Alternately, instead of writing the log file to a common location and risk all users on the system having access to it, the drwtsn32.exe application can be run and a new log and crash dump location can be specified.	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control Full Control RWXD	Replace
%SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\HTML Help	Administrators SYSTEM Users	Full Control Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\All Users\Application Data\Microsoft\Media Index	Administrators SYSTEM Users Users	Full Control Full Control R X Create files, Create folders, Write attributes, Write extended attributes, read permissions (this folder only) Write (Subfolders and files)	Replace
%SystemDrive%\Documents and Settings\All Users\Documents (Shared Documents) NOTE: When viewing the %AllUsersProfile% folder in Windows Explorer, the Documents subfolder appears as "Shared Documents."	Administrators SYSTEM Users	Full Control Full Control R X	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\All Users\Documents (Shared Documents)\desktop.ini	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users	Full Control Full Control Full Control R X	Replace
<p>%SystemDrive%\Documents and Settings\Default User</p> <p>NOTE: If WINDOWS 2003 has been reinstalled over another copy of the operating system, additional Default User profile folders will be created in the Documents and Settings folder. Typically, the new profile is called Default User.WINDOWS or Default User.COMPUTERNAME. Prior copies of the Default User folder, although still existing, will not be used. Unlike the All Users profile, Default User does not have an associated environment variable, Therefore, the currently-used profile should be specified in this template entry if different than Default User. To determine the Default User profile currently being used, see the HKLM\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\DefaultUserProfile registry key value.</p>	Administrators SYSTEM Users	Full Control Full Control RX	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemDrive%\Documents and Settings\LOCAL SERVICE	Administrators LOCAL SERVICE SYSTEM	Full Control Full Control Full Control	Replace
%SystemDrive%\Documents and Settings\NETWORK SERVICE	Administrators NETWORK SERVICE SYSTEM	Full Control Full Control Full Control	Replace
%SystemDrive%\Program Files	Administrators Users CREATOR OWNER (subfolders & files) SYSTEM	Full Control RWX Full Control Full Control	Propagate
%SystemDrive%\Program Files\Resource Kit (Servers and Domain Controllers)	Administrators SYSTEM	Full Control Full Control	Replace
%SystemDrive%\Temp	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users	Full Control Full Control Full Control Traverse folder, Create files, Create folders (folders & subfolders)	Replace
%SystemRoot%	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subfolders & files) Full Control RX	Replace
%SystemRoot%\\$HF_MIG\$	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\\$NtServicePackUninstall\$	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\\$NtUninstall* (all uninstall folders)	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\debug	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users	Full Control Full Control Full Control RX	Propagate
%SystemRoot%\debug\UserMode	Administrators SYSTEM Users Users	Full Control Full Control Traverse folder, List Folder, Create files (folder only) Write data, Append data (files only)	Propagate
%SystemRoot%\debug\UserMode\userenv.log	Administrators SYSTEM Users	Full Control Full Control Write data, Append data	Replace
%SystemRoot%\Installer	Administrators SYSTEM Users	Full Control Full Control R X	Replace
%SystemRoot%\NTDS (Domain Controllers only) (Active Directory database folder – the %SystemRoot% portion of the path name may need to be changed depending on where the default Active Directory folder is located)	Administrator Users SYSTEM	Full Control RX Full Control	Replace
%SystemRoot%\Prefetch	Administrators Administrators SYSTEM	Full Control (This folder only) R X (Files only) Full Control (Files only)	Replace
%SystemRoot%\regedit.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Registration	Administrators SYSTEM Users	Full Control (This folder and files) Full Control (This folder and files) R (This folder and files)	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\Registration\CRMlog	Administrators Creator Owner SYSTEM Users Users	Full Control Full Control (Subfolders and files only) Full Control Traverse folder, List folder, Read attributes, Read extended attributes, Create files, Read Permissions (This folder only) Read data, Read attributes, Read extended Attributes, Write data, Append data, Write Attributes, Write extended attributes, Delete, Read permissions (Files only)	Replace
%SystemRoot%\Repair	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\Security	Administrators CREATOR OWNER (subfolders & files) SYSTEM	Full Control Full Control Full Control	Replace
%SystemRoot%\Temp	Administrators CREATOR OWNER (subfolders & files) SYSTEM Users	Full Control Full Control Full Control Traverse folder, Create files, Create folders (This folders & subfolders)	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\System32 Folder, subfolders, and files	Administrators Users CREATOR OWNER (subfolders and files) SYSTEM	Full Control R X Full Control Full Control	Replace
%SystemRoot%\System32\arp.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\at.exe (This utility is obsolete and should be removed)	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\ciadv.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\compmgmt.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\devmgmt.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\dfgr.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\diskmgmt.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\eventvwr.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\fsmgmt.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\gpedit.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\iusrmgr.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\nbtstat.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\netsh.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\netstat.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\nslookup.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\Ntbackup.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\ntmsmgr.msc	Administrators SYSTEM	Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\System32\ntmsoprq.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\perfmon.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\rcp.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\reg.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\SYSTEM32\regedt32.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\regini.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\rexc.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\route.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\rsh.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\RsoP.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\secedit.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\secpol.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\services.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\systeminfo.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\tftp.exe	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\wmimgmt.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\Com\comexp.msc	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\CONFIG	Administrators SYSTEM	Full Control Full Control	Replace
%SystemRoot%\System32\CONFIG\AppEvent.evt %SystemRoot%\System32\CONFIG\SecEvent.evt %SystemRoot%\System32\CONFIG\SysEvent.evt	Administrators (Auditor's group) SYSTEM	R X Full Control Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\System32\dlcache	Administrator CREATOR OWNER SYSTEM	Full Control Full Control (Subfolders and files only) Full Control	Replace
%SystemRoot%\System32\GroupPolicy	Administrator Users SYSTEM	Full Control R X Full Control	Propagate
%SystemRoot%\System32\ias	Administrator CREATOR OWNER SYSTEM	Full Control Full Control Full Control	Replace
%SystemRoot%\System32\MSDTC	Administrator NETWORK SERVICE SYSTEM	Full Control RWX Full Control	Propagate
%SystemRoot%\System32\NTMSData	Administrator SYSTEM	Full Control Full Control	Propagate
%SystemRoot%\System32\Setup	Administrator SYSTEM Users	Full Control Full Control R X	Propagate
%SystemRoot%\System32\spool\Printers	Administrator CREATOR OWNER (subfolders & files) SYSTEM Users	Full Control Full Control Full Control Traverse folder, Read attributes, Read extended attributes, Create files, Create folders (This folder & subfolders)	Replace
%SystemRoot%\SYSVOL (Domain Controllers only)	Administrator Users SYSTEM	Full Control RX Full Control	Replace

FOLDER OR FILE	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
%SystemRoot%\SYSVOL\domain\Policies (Domain Controllers only) (The %SystemRoot% portion of the path may need to be changed depending on where the default Active Directory folder is located)	Administrator Users SYSTEM	Full Control RX Full Control	Replace

This page intentionally left blank.

APPENDIX B. REQUIRED REGISTRY KEY PERMISSIONS

Registry keys not explicitly listed below are assumed to inherit the permissions of their parent key if they already have **Inherit from parent the permission entries that apply to child objects** checked in their DACL. Keys with **Do not allow permissions on this key to be replaced** selected are explicitly excluded from security configuration and retain their original permissions. In the table, the term “Propagate” indicates that the **Propagate inheritable permissions to all subkeys** radio button should be enabled while “Replace” indicates that the Replace existing permissions on all subkeys with inheritable permissions radio button should be enabled. “Ignore” means that the key is excluded from configuration.

On Domain Controllers the Group “Users” should be replaced with “Authenticated Users.”

The following notation is used in this section of the security templates:

CLASSES_ROOT indicates HKEY_CLASSES_ROOT hive

MACHINE indicates HKEY_LOCAL_MACHINE hive

USERS indicates HKEY_USERS hive

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
CLASSES_ROOT\	Administrators CREATOR OWNER (Subkeys only) SYSTEM Users	Full Control Full Control Full Control Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Read	Replace
MACHINE\SOFTWARE (include all subkeys)	Administrators CREATOR OWNER (subkeys only) SYSTEM Users	Full Control Full Control Full Control read(QENR)	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
MACHINE\SOFTWARE\Microsoft\Cryptogropy\Calais	Administrators Creator Owner LOCAL SERVICE SYSTEM Users	Full Control Full Control (Subkeys only) Query value, Set Value, Create subkey, Enumerate subkeys, Notify, Delete, Read permissions Full Control read(QENR)	Replace
MACHINE\SOFTWARE\Microsoft\MSDTC	Administrators NETWORK SERVICE SYSTEM Users	Full Control Query value, Set Value, Create subkey, Enumerate subkeys, Notify, Read permissions Full Control read(QENR)	Propagate
MACHINE\SOFTWARE\Microsoft\MSDTC\Security\XAKey	Administrators NETWORK SERVICE SYSTEM	Full Control Query value, Set Value, Create subkey, Enumerate subkeys, Notify, Read permissions Full Control	Replace
MACHINE\SOFTWARE\Microsoft\NetDDE	Administrators Creator Owner SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Group Policy	Administrators Users SYSTEM	Full Control read(QENR) Full Control	Propagate
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer	Administrators Users SYSTEM	Full Control read(QENR) Full Control	Propagate
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies	Administrators Users SYSTEM	Full Control read(QENR) Full Control	Propagate
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings	Administrators Users	Full Control read(QENR)	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Telephony	Administrators Creator Owner LOCAL SERVICE NETWORK SERVICE Users SYSTEM	Full Control Full Control (Subkeys only) Full Control Full Control read(QENR) Full Control	Replace
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Asr\Commands	Administrators Backup Operators CREATOR OWNER SYSTEM Users	Full Control Query, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control (Subkeys only) Full Control Read (QENR)	Replace
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib	Administrators CREATOR OWNER INTERACTIVE NETWORK SERVICE SYSTEM	Full Control Full Control (Subkeys only) read(QENR) read(QENR) Full Control	Replace
MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SecEdit	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subkeys only) Full Control read(QENR)	Replace
MACHINE\SYSTEM\controlsetXXX (XXX represents the control set number 001-010)	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subkeys only) Full Control read(QENR)	Propagate

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
MACHINE\SYSTEM\CurrentControlSet\Control\Class	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subkeys only) Full Control read(QENR)	Propagate
MACHINE\SYSTEM\CurrentControlSet\Control\Network	Administrators LOCAL SERVICE NETWORK SERVICE SYSTEM Users	Full Control Full Control Full Control Full Control read(QENR)	Replace
MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg (The Exchange Enterprise Servers group can have full control on Domain Controllers and Exchange server)	Administrators Backup Operators LOCAL SERVICE	Full Control read(QENR) (This key only) read(QENR)	Replace
MACHINE\SYSTEM\CurrentControlSet\Control\Wmi\Security	Administrators Administrators CREATOR OWNER SYSTEM	read(QENR) Full Control (This key only) Full Control (Subkeys only) Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles	Administrators CREATOR OWNER SYSTEM Users	Full Control Full Control (subkeys only) Full Control read(QENR)	Propagate
MACHINE\SYSTEM\CurrentControlSet\Services\AppMgmt\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\ClipSrv\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\CryptSvc\Security	Administrators SYSTEM	Full Control Full Control	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
MACHINE\SYSTEM\CurrentControlSet\Services\DNSCache	Administrators LOCAL SERVICE Network Configuration Operators NETWORK SERVICE SYSTEM Users	Full Control Full Control Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control Full Control read(QENR)	Propagate
MACHINE\SYSTEM\CurrentControlSet\Services\Ersvc\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\IRENUM\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Netbt	Administrators LOCAL SERVICE Network Configuration Operators NETWORK SERVICE SYSTEM Users	Full Control Full Control Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control Full Control read(QENR)	Propagate
MACHINE\SYSTEM\CurrentControlSet\Services\Netdde\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Netdddsdm\Security	Administrators SYSTEM	Full Control Full Control	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess	Administrators LOCAL SERVICE Network Configuration Operators NETWORK SERVICE SYSTEM Users	Full Control Full Control Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control Full Control read(QENR)	Propagate
MACHINE\SYSTEM\CurrentControlSet\Services\Rpcss\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Samss\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Scarddrv\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Scardsvr\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\PermittedManagers	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ValidCommunities	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Stisvc\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\SysmonLog\Log Queries	Administrators Creator Owner NETWORK SERVICE SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Full Control read(QENR)	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Tapisrv\Security	Administrators SYSTEM	Full Control Full Control	Replace

REGISTRY KEY	USER GROUPS	RECOMMENDED PERMISSIONS	INHERIT METHOD
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip	Administrators LOCAL SERVICE Network Configuration Operators NETWORK SERVICE SYSTEM Users	Full Control Full Control Query Value, Set Value, Create Subkey, Enumerate, Notify, Delete, Read permissions Full Control Full Control read(QENR)	Propagate
MACHINE\SYSTEM\CurrentControlSet\Services\W32time\Security	Administrators SYSTEM	Full Control Full Control	Replace
MACHINE\SYSTEM\CurrentControlSet\Services\Wmi\Security	Administrators SYSTEM	Full Control Full Control	Replace
USERS\.DEFAULT	Administrator CREATOR OWNER SYSTEM Users	Full Control Full Control (Subkeys only) Full Control Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Read	Replace
USERS\.DEFAULT\Software\Microsoft\NetDDE	Administrator Creator Owner SYSTEM	Full Control Full Control (Subkeys only) Full Control	Replace
USERS\.DEFAULT\Software\Microsoft\SystemCertificates\Root\ProtectedRoots	Administrator SYSTEM Users	Full Control Full Control read(QENR)	Replace

This page is intentionally left blank.

APPENDIX C. RELATED PUBLICATIONS

Government Publications

Department of Defense (DOD) Directive 8500.1, "Information Assurance", October 2002.

Department of Defense (DOD) Instruction 8500.2, "Information Assurance (IA) Implementation", February 2003.

Defense Information Systems Agency (DISA)/Chief Information Officer, Memorandum for Distribution, "DISA Standard Computer Configurations," Version 1999-A, November 1998.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," July 1996.

Defense Information Systems Agency (DISA)/Defense Information Services Organization (DISO) Naming Convention Standards, March 1994.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Active Directory," Version 1.0, December 2000.

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Group Policy," Version 1.1, September 2001.

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 File and Disk Resources," Version 1.0, 19 April 2001.

National Security Agency (NSA), "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set," Version 1.2, December 2002.

National Security Agency (NSA), "Guide to Securing Microsoft Windows NT Networks," Version 4.2, 18 September 2001.

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," 4 September 1990.

Air Force Systems Security Instruction (AFSSI) 5102, "The Air Force Computer Security (COMPUSEC) Program," 23 September 1997.

Air Force Systems Security Memorandum (AFSSI) 5002, "Control/Access Protection," 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.

General Accounting Office Report to Congressional Requester (GAO/AIMD-96-84), "Information Security Computer Attacks at Department of Defense Pose Increasing Risks."

Field Security Operations Publications

DISA Computing Services Security Handbook, Version 3, 1 December 2000.

Desktop Application STIG, V1R1, 22 November 2002.

Network Infrastructure STIG, V5R2, 29 Sept 2003.

Web Server STIG, V4R1, 31 August 2003.

Commercial and Other Publications

Microsoft Solutions for Security, Windows Server 2003 Security Guide, 2003

Microsoft Solutions for Security, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, 2003

Web Sites

DISA –	http://www.disa.mil
DISA Datahouse –	https://datahouse.disa.mil
DISA Field Security Operations –	https://guides.ritchie.disa.mil
DISA Information Assurance–	https://iase.disa.mil http://iase.disa.smil.mil (SIPRNET)
DOD-CERT –	http://www.cert.mil http://www.cert.smil.mil/antivirus/updates.htm (SIPRNET)
Mergent (encryption software) –	http://www.mergent.com
Microsoft's Knowledge Base Web Site –	http://www.microsoft.com/kb/
NCSA –	http://www.ncsa.com
Netscape –	http://wp.netscape.com/security/index.html
RSA Data Systems (encryption software) –	http://www.rsa.com
Symantec Corporation (ESM)	http://www.symantec.com
Vulnerability Compliance Tracking System (VCTS) –	https://vms.disa.mil
Vulnerability Compliance Tracking System (VCTS) (Secret and Confidential) –	https://vms.disa.smil.mil

This page is intentionally left blank.

APPENDIX D. WINDOWS SERVER 2003 - INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

This appendix lists all IAVM bulletins applicable to Windows Server 2003, as of the effective date of this document, including applications that may be installed. This list is complete as of January 2003. Refer to the current Windows 2003 checklist for the most up-to-date listing.

IAVM BULLETINS FOR WINDOWS SERVER 2003:

IAVM BULLETINS FOR SERVICES AND APPLICATIONS

DOD-CERT IAVM Alerts – Windows OS

IAVM 2003-A-0012 – Microsoft RPCSS DCOM Interface Buffer Overflow

IAVM 2003-A-0017– Microsoft Messenger Service Buffer Overflow Vulnerability

DOD-CERT IAVM Bulletins – Windows OS

IAVM 2003-B-0004 – Microsoft Internet Explorer HTML Converter Buffer Overflow
Vulnerability

IAVM 2003-B-0006 – Microsoft Authenticode Verification Vulnerability

DOD-CERT IAVM Technical Advisories - Windows OS

(None)

DOD-CERT IAVM Alerts - Microsoft Applications

IAVM 2001-A-0012 – Malformed Excel or PowerPoint Document can Bypass Macro Security

IAVM 2003-A-0001 (V1) – Multiple Vulnerabilities with Microsoft SQL Server

DOD-CERT IAVM Bulletins – Microsoft Applications

(None)

DOD-CERT IAVM Technical Advisories - Microsoft Applications

IAVM 1999-T-0016 - Microsoft Excel Symbolic Link (SYLK) Vulnerability

IAVM 2000-T-0007 - Microsoft Office 2000 UA ActiveX Control

IAVM 2000-T-0010/0010.1 - Microsoft “IE Script” and “Office 2000 HTML Script”

IAVM 2000-T-0012 - Office 2000 HTML Object Tag

IAVM 2000-T-0014 - Excel Register.ID Function

IAVM 2003-T-0019 – Microsoft WordPerfect Converter Buffer Overrun Vulnerability

DOD-CERT IAVM Alerts (IAVM) – Web Servers

(None)

DOD-CERT IAVM Bulletins (IAVB) – Web Servers

(None)

DOD-CERT IAVM Technical Advisories – Web Servers

IAVM 2003-T-0003 – Apache Web Server Multiple Denial of Service Vulnerabilities

IAVM 2003-T-0009 – Various Vulnerabilities in Apache Web Server

IAVM 2003-T-0012 – Apache Web Server Multiple Denial of Service Vulnerabilities

DOD-CERT IAVM Alerts (IAVM) – Web Browsers

IAVM 2003-A-0014 – Multiple Vulnerabilities in Microsoft Internet Explorer

DOD-CERT IAVM Bulletins (IAVB) – Web Browsers

IAVM 2000-B-0002 – Netscape Navigator Improperly Validates SSL Sessions

DOD-CERT IAVM Technical Advisories – Web Browsers

IAVM 2002-T-0003 – VBScript in IE allows Web pages to read local files

DOD-CERT IAVM Alerts (IAVM) - Other Applications

IAVM 2003-A-0008 – Multiple Overflow Vulnerabilities in Snort

DOD-CERT IAVM Bulletins (IAVB) - Other Applications

(None)

DOD-CERT IAVM Technical Advisories - Other Applications

IAVM 2000-T-0015 - BMC Best/1 Version 6.3 Performance Management System Vulnerability

IAVM 2001-T-0009 – Norton AntiVirus LiveUpdate Host verification vulnerability

IAVM 2003-T-0006 – Vulnerabilities in McAfee ePolicy Orchestrator Agent

APPENDIX E. QUICK START CHECKLIST

Use this checklist as step-by-step guidance to comply with STIG requirements when installing a new SERVER. The FSO Windows 2003 SRR Checklists, FSO Windows 2003 Addendum, and Windows Server 2003 Guide should be referred to in performing the installation.

Prior to installation, ensure the following:

The location of all equipment is in a secured area in accordance with DoD requirements.

A separate partition exists for the operating system and applications.

No previously installed operating system exists, that is not C2 or NIAP compliant.

Remove any modems installed.

Assemble the installation software, current Service Pack(s), and Hotfix(s).

Current approved service pack
Check for additional hotfixes issued.

Obtain Norton Anti-Virus or McAfee Virus Shield software and the most current signature file.

For servers that will have additional functionality, ensure the applicable application software, service pack(s), and hotfix(s) are obtained (e.g., IIS, SQL Server, Terminal Server, etc.).

Obtain all IAVM bulletin information for Windows 2003 and applicable applications.

Installation:

Follow these steps to ensure STIG compliance when installing a Windows Server 2003.

The new Server (DC or standalone) is **not connected** to the network until after configured to STIG compliance.

NOTE: Additional DCs will need network connectivity to access Active Directory in order to be promoted.

Install Windows according to manufacturer instructions and site configuration requirements.

- Format or convert the system's hard drive to the NTFS file system.

Install current service pack and applicable hotfixes.

Install Norton Anti-Virus or McAfee Virus Shield software and the most current signature file.

Create system state backups. (Back up Active Directory on Domain Controllers)

- Performing a full backup may be advisable at this point if additional applications are to be installed.

Configure Security settings in accordance with the Windows Server 2003 Guide and the FSO Addendum. (A Server 2003 configuration file is available from FSO that can be used with Microsoft's Security Configuration MMC snap-in, or imported into a Group Policy)

- Rename the built-in Administrator account.
 - Ensure a complex password is assigned.
- Set screen saver settings (set prior to creating accounts).
 - Current User
 - Default User
- *Create Administrator level accounts.
- *Create Auditors group.
- Configure Guest account.
 - Rename.
 - Assign a 14-character complex password.

- Disable.
- *Create a decoy Administrator account.
 - Disable.
 - Assign a complex password.
 - Assign group membership to a Guest group.
- Set the User Account settings.
 - Maximum password age
 - Minimum password age
 - Minimum password length
 - Password uniqueness
 - Account lockout
 - Bad logon attempts
 - Bad logon counter reset
 - Lockout duration
 - Logon before password change
 - Forced disconnect when logon hours expire (DCs only)
- *Configure FTP services.
 - Enter Warning Banner into registry (NT).
 - If FTP is not to be used:
 - DISABLE FTP services
 - If FTP is being used:
 - Configure for one-way communication.
 - Configure to not allow anonymous logons.
 - Configure to not allow access to root/system drive.
- Remove any DOS directory (On boxes that have been upgraded several times).
- Remove the POSIX files.

- *Copy the ENPASFLT.DLL to %root%\System32 directory.
- Configure the Registry.
- Set the file and directory permissions (access control list).
 - System files
 - Event logs
- Set the registry key permissions (access control list).
- Set the appropriate printer share permissions for locally installed printers.
- Configure installed services.
 - Remove Remote Shell services.
 - Disable unneeded Scheduler/Task Scheduler services.
 - Disable Simple TCP/IP services.
 - Disable Telnet services.
 - Remove Fingerd services.
 - Remove RCMD services.
 - Disable SNMP services if not required.
- Set DCOM settings, if applicable.
- Disable IP forwarding, if applicable.
- Set Recycle Bin to Remove Files Immediately on Delete. (Servers)
- Set User Rights policy configuration.
- Set Event log settings.
 - Retention settings (server, workstation)
 - Log size settings (server, workstation)
- Enable Auditing
 - Enable auditing.
 - Set the auditing configuration.
 - Set file and directory auditing.

- Set registry auditing.
- *Create User Accounts, if applicable.
- *Install and configure an intrusion detection product (all servers).
- *Install and configure applications, if applicable.
- *Perform a sample SRR.
 - Refer to the *Microsoft Windows security guides* and the *Windows 2003 Addendum*.
 - Fix any findings.

Prior to connecting to the network, ensure the following:

Register with VMS.

SAs
Servers

A CMOS password is set and the boot sequence is from the hard disk only.

This page is intentionally left blank.

APPENDIX F. GLOSSARY OF TERMS

ACE	Access Control Entry
ACL	Access Control List
AIS	Automated Information System
AS	Authentication Server
BDC	Backup Domain Controller
C3I	Command, Control, Communications, and Intelligence
C&A	Certification and Accreditation
CCB	Configuration Control Board
CD	Compact Disk
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Authentication Protocol
CIFS	Common Internet File System
CIS	The Center for Internet Security
CISS	Center for Information Systems Security
CMOS	Complementary Metal-Oxide Semiconductor
COE	Common Operating Environment
COTS	Commercial Off-The-Shelf
DAA	Designated Approving Authority
DAC	Discretionary Access Control
DACL	Discretionary Access Control List
DCTF	DISA Continuity of Operations and Test Facility
DECC	Defense Enterprise Computer Center
DECC-D	Defense Enterprise Computer Center - Detachment
DHCP	Dynamic Host Configuration Protocol
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency Instruction
DLL	Dynamic Link Library
DNS	Domain Name Server
DOD	Department of Defense
DOD-CERT	Department of Defense Computer Emergency Response Team
DODICS	Department of Defense Interest Computer System
DODIG	DOD Inspector General
DoS	Denial of Service
DOS	Disk Operating System
ERD	Emergency Repair Disk
ESM	Enterprise Security Manager
FAT	File Allocation Table
FTP	File Transfer Protocol

GAO	General Accounting Office
GIF	Graphics Interchange Format
GNOSC	Global Network Operations and Security Center
GOTS	Government-Off-The-Shelf
HPFS	High Performance File System
HTTP	Hyper Text Transport Protocol
I&A	Identification and Authentication
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAW	In Accordance With
IE	Internet Explorer
IETF	Internet Engineering Task Force
IG	Inspector General
IIS	Internet Information Server
INFOSEC	Information Security
INFOWAR	Information Warfare
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IS	Information System
ITA	Intruder Alert
JID	Joint Intrusion Detector
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
LM	LanManager
LSA	Local Security Authority
MAPI	Mail Application Programming Interface
MD5	Message Digest Version 5
MOA	Memorandum of Agreement
NCSC	National Computer Security Center
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NIAP	National Information Assurance Partnership
NIC	Network Interface Card
NID	Network Intrusion Detector
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network
NNTP	Network News Transfer Protocol
NOSC	Network Operations and Security Center
NSA	National Security Agency
NSO	Network Security Officer
NTFS	NT File System
OS	Operating System

PC	Personal Computer
PCT	Private Communications Technology
PDC	Primary Domain Controller
POC	Point-of-Contact
POP	Point-of-Presence
POSIX	Portable Operating System Interface for Computing Environments
PPP	Point-to-Point Protocol
RAM	Random Access Memory
RAS	Remote Access Service
RCC	Regional Control Center
RCERT	Regional CERT
RISC	Reduced Instruction Set Computer
RNOSC	Regional Network Operations and Security Center
RPC	Remote Procedure Call
RSA	Regional Support Activity
RSC	Regional Service Center
SA	System Administrator
SAM	Security Accounts Manager
SBU	Sensitive but Unclassified
SCSI	Small Computer Systems Interface
SID	Security Identifier
SIPRNet	Secret Internet Protocol Router Network
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMS	Systems Management Server
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOP	Standard Operating Procedure
SRM	Security Reference Monitor
SSL	Secure Sockets Layer
SSO	Systems Support Office
STIG	Security Technical Implementation Guide
TAPI	Telephony Applications Programming Interface
TASO	Terminal Area Security Officer
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
URL	Universal Resource Locator

VAAP	Vulnerability Analysis and Assistance Program
VCTS	Vulnerability Compliance Tracking System
VGA	Video Graphics Array
VMS	Vulnerability Management System
WAN	Wide Area Network
WINS	Windows Internet Name Service
WWW	World Wide Web