WINDOWS NT/2000/XP

ADDENDUM

Version 4, Release 1

26 FEBRUARY 2004

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

Page

SUMMARY OF CHANGES

- General: Reformatted the document to consolidate or remove several sections and revised section numbering.
- General: Added PDI numbers and Category codes to all requirements that have a corresponding SRR check.
- Revised Section 1, *Introduction.*
- Revised *Section 2.1, Gold Standard*, to include a discussion of the Gold Disk.
- Added new *Section 2.2, Additional Gold Standard Settings.*
- Revised *Section 3.1, Permitted Operating Systems.*
- Revised *Section 4.3, Registry Settings.* Added security option settings for XP.
- Inserted new *Section 4.3.3, Group Policy Background Refresh.*
- Added a new note to *Section 4.5.3, Password Policy.*
- Added new *Section 4.5.4, Unsigned Driver Installation Behavior*.
- Revised *Section 5, Account Policies and User Rights.* Included new rights related to XP.
- Added new *Section 5.2, Windows XP Built-in Accounts.*
- Added new *Section 5.3, Dormant Accounts.*
- Revised *Section 6.3, Audit Failure Procedures.* Added automatic log backup procedure.
- Revised *Section 6.5, Registry Audit Settings*.
- Revised *Section 7.1, DOD Physical Security Requirements* to include a restriction for Remote Access Cards on Domain Controllers.
- Added new *Section 7.2.1, Mobile USB Disk Devices (WIN2K and XP).*
- Revised *Section 7.4, Installed Services*. Added additional services to be disabled to conform with the CIS Baseline standard for WIN2K. Changed the ordering of the services to match the way they appear in the Windows Services applet.

- Inserted new *Section 7.6, Plug and Play (WIN2K and XP).*
- Inserted new *Section 7.7, USB Ports (WIN2K and XP).*
- Revised *Section 8.2, Removing Unneeded Applications.*
- Added new *Section 8.2.1, Microsoft Zone Internet Games.*
- Added new *Section 8.2.2, MSN Explorer (XP).*
- Added new *Section 8.2.3, IIS Components (XP).*
- Added new *Section 8.3, Application Security – Microsoft Applications.*
- Added new *Section 8.3.1, Internet Explorer Policy Settings (WIN2K and XP).*
- Added new *Section 8.3.2, Terminal Services (XP).*
- Added new *Section 8.3.3, Windows Installer (WIN2K and XP).*
- Added new *Section 8.3.4, Windows Messenger.*
- Added new *Section 8.4, Application Security – Other Applications.*
- Inserted new *Appendix F, Additional Gold Standard Settings (WIN2K).*
- Revised *Appendix A, Related Publications.*
- Revised *Appendix B, Windows NT – Information Assurance Vulnerability Management (IAVM) Compliance.*
- Revised *Appendix C, Windows 2000 – Information Assurance Vulnerability Management (IAVM) Compliance.*
- Inserted new *Appendix D, Windows XP – Information Assurance Vulnerability Management (IAVM) Compliance.*
- Revised *Appendix G, Quick Start Checklist,* to include XP.
- Revised *Appendix H, List of Acronyms.*

1. INTRODUCTION

1.1 Background

This Addendum to the NSA Guide to Securing Microsoft Windows NT Networks (NSA Windows NT Guide) and NSA Guides to Securing Windows 2000 and XP was developed to enhance the confidentiality, integrity, and availability of sensitive Department of Defense (DOD) Automated Information Systems (AISs) using the Windows NT, 2000, and XP operating systems.

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

- NSA Guide to Securing Microsoft Windows NT Networks, 18 September 2001, Version 4.2 (NSA Windows NT Guide.)
- NSA Guide to Securing Windows 2000 Active Directory, December 2000, Version 1.0
- NSA Guide to Securing Windows 2000 Group Policy, September 2001, Version 1.1
- NSA Guide to Securing Windows 2000 Group Policy: Security Configuration Tool Set, December 2002, Version 1.2
- NSA Guide to Securing Windows 2000 File and Disk Resources, 19 April 2001, Version 1.0
- NSA Guide to Securing Windows XP, October 2002, Version 1.0 (NSA XP Guide.)

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 NSA Windows 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.

Because customer-driven requirements and site operating environments are so varied, a **cookie-cutter** approach to security is not practical. The Information Assurance Manager (IAM), Information Assurance Officer (IAO), Terminal Area Security Officer (TASO), Network Security Officer (NSO), and System Administrators (SA), in cooperation with customers, must weigh security with operational necessities. This document in addition to the NSA Windows Guides listed above, specifies the minimum requirements for securing the Windows NT, Windows 2000, and Windows XP operating systems. Each site may implement additional security measures as necessary to optimize the system's overall operation. If guidelines must be modified for the proper and secure operation of an operating environment and infrastructure, the IAO will ensure the system's overall secure operation.

NOTE: Unless otherwise specified, these requirements apply equally to servers and workstations.

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 Windows NT/2000/XP operating systems (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 have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

1.6 DISA Gold Standard

The *Gold Standard* was developed with Information Technology (IT) security as well as operational impact in mind. Operational impact includes required security settings, which will disable or cause loss of functionality of the information system or application. Operational impact cannot override security; the operational impact must be weighed against the risk of not implementing a security control. The Gold Standard is the establishment of a minimum-security baseline applied to DOD systems. The Gold Standard provides a high level of assurance that the functionality of the information system or application will not be adversely impacted as a result of implementing the Gold Standard settings. Security controls designated as *Platinum Standard* provide a higher level of security assurance but may impact operations. All requirements within this document are to be considered a Gold Standard unless denoted as a Platinum Standard on the applicable checklist.

1.7 STIG Distribution

Parties within the DOD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. 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**.

1.8 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.

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 Gold Standard

The Gold Standard is a baseline level of security that is the minimum required to attach a system to a production or development network, unless the individual site requires a more secure standard. A consortium of government and civilian organizations that included DISA Field Security Operations (FSO), the National Security Agency (NSA), the National Institute of Standards and Technology (NIST), the Center for Internet Security (CIS), and many others developed it. Settings were chosen with the intent to configure the system to be as secure as possible and yet maintain a stable environment that would not impact the applications that would run on it. It is a starting point upon which a site can build additional levels of tighter safeguards. As of this writing, a baseline has been developed for Windows 2000 Professional and for Windows 2000 Servers, and work is ongoing for Windows XP and Windows 2003.

The Gold Standard is not meant as a measure for Certification and Accreditation. It is not a level that is sufficient to conform to STIG requirements.

For the purpose of conforming to STIG requirements, DOD organizations will configure systems to meet what it calls a Platinum Standard, which equates to the current requirements in the NSA Windows Guides and this *Addendum*.

FSO has created a 'Gold Disk' for Windows 2000 Professional, Windows 2000 Server, and Windows XP. The Gold Disk can be used to bring a system to the current level for service packs and hot fixes. In addition it will configure most of the security settings required by the appropriate STIG to meet the Gold Standard or Platinum Standard. The Gold Disk can be used to secure, maintain, and validate STIG and IAVM compliance.

2.2 Additional Gold Standard Settings

There are several Gold Standard settings recommended by the CIS Baseline configurations for Windows operating systems that do not appear in the NSA security guides. These settings are listed in *Appendix F* of this document and are included in the FSO Gold and Platinum configurations.

2.3 Security Controls

Windows NT/2000/XP are operating systems in which the typical OS function and networking are integrated. They provide 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 NT/2000/XP workstation or server is configured to provide compliance with the security required by *Department of Defense Directive 8500.01 (DODD), Department of Defense Instruction Directive 8500.02 (DODI)* 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 III) 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. They are most often found in the system directories but could be in other locations. The SA should maintain thee 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.

- *(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 will be baselined and compared.*

- *(1.025: CAT II) The IAM will ensure the DOD servers will use host-based Intrusion Detection Systems (IDSs) on all systems.*

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.

2.3.1 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 of originated within DOD:
>
> (i.) Comply with the evaluation and validation requirements of National Security Telecommunications and Information Systems Security Policy Number 11 and;
>
> (ii.) 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**.

2.4 Patch Control

Maintaining the security of a Windows NT/2000/XP system requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch (**hot fix**) 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 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.

2.4.1 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

2.4.2 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. Windows NT cannot use it.

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 system administrators 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:

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

2. 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

The DOD SUS URLs will not respond in a browser. Information about the DOD SUS servers can be found at:

http://dodsus.csd.disa.mil/client/install.htm or
http://dodsus.csd.disa.smil.mil/client/install.htm.

2.5 Administrative Tools

The use of automated vulnerability and intrusion detection products are recommended to assess the vulnerability of the sites' Windows NT/2000/XP operating systems. Microsoft has incorporated several utilities to assist in assessing Windows NT/2000/XP vulnerabilities.

- *(1.016: CAT III) For Windows NT, the IAO or Terminal Area Security Officer (TASO) will use the Security Configuration Manager, as described in Chapters 3 through 12 of the NSA NT Guide.*

- *(1.016: CAT III) For Windows 2000/XP, the IAO or TASO will use the Security Configuration Tool Set, as described in the NSA WIN2K guide entitled "Guide for Securing Windows 2000 Group Policy: Security Configuration Tool Set", and the NSA XP Guide.*

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

This page is intentionally left blank.

3. SECURING THE WINDOWS NT/2000/XP OPERATING SYSTEM

3.1 Permitted Operating Systems

Windows NT 4.0, SP6a and later, can be configured to C2 compliance for providing a maximum level of security when networked to other platforms. C2 requirements will be used to evaluate the strength of a Windows NT system.

In February 2003, Windows 2000 was NIAP certified with Service Pack 3 and security hot fix Q326886. Service Pack 4 has superseded Service Pack 3 and related hot fixes.

- *(5.003: CAT II) The IAO will ensure that the system will boot only to STIG compliant operating systems.*

- *(2.005: CAT II) The IAO will ensure that Windows 2000 has the most current Service Pack installed.*

In June 2003, Microsoft dropped support for Windows NT 4.0 Workstation. After 30 June 2004, Microsoft will no longer evaluate this operating system for security vulnerabilities, and will not release any further hot fixes. Microsoft has also stated that they will drop normal unpaid support for Windows NT 4.0 Server on 31 December 2003, but will continue to provide paid support and release security related hot fixes until 31 December 2004.

- (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 WINDOWS 2000/XP POLICIES

4.1 Windows NT/2000/XP Registry Access Policy

Implementing security measures within the Windows NT/2000/XP 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 NT/2000/XP 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 System Administrator should modify registry settings.

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

NOTE: An Emergency Repair Disk (ERD) 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" ERD should be made and maintained. If possible, a current backup that includes the registry should be available for all critical servers.

4.2 Windows 2000/XP Active Directory/Group Policy Access Policy

Most security measures in Windows 2000 are implemented using Group Policies that reside in the Active Directory. Unlike the security settings in Windows NT that affect a single machine, 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. Protecting the Active Directory and Group-level policies from being altered, by unauthorized or untrained persons, is essential.

- *(1.006: CAT II) The IAO will ensure that only trained, authorized System Administrators 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 2000/XP guides for "Group Policy" and "Active Directory" are enforced.*

4.3 Registry Settings

On Windows NT machines, the following security settings are made directly in the Registry using the **regedt32.exe** editing program. On Windows 2000/XP machines, provision has been made to modify some of these settings through the Microsoft Management Consol (MMC), using Security Configuration and Analysis, and Policy snap-ins. Follow the general guidance for modifying Security Options in the *NSA Security 2000 Guide* for *"Security Configuration Tool Set"* and the NSA XP Guide. 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 *NSA Windows Guides.*

NOTE: On Windows 2000/XP machines, load the updated Security Options File, following instructions in the appropriate 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 NT/2000/XP 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 to a Windows NT/2000/XP machine 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.*

Windows NT:

The registry key should be set as follows:

Hive: HKLM

Key: \System\CurrentControlSet\Services\Rasman\Parameters

Name: DisableSavePassword

Type: REG_DWORD

Value: 1

- Select the **HKEY_LOCAL_MACHINE** on the local machine window.
- Navigate down the **System\CurrentControlSet\Services\Rasman** path, double clicking on each key along the way.
- Select the **Parameters** key.
- Select **Add Value**… from the **Edit** menu.
- Enter **DisableSavePassword** for **Value Name**.
- Select **REG_ DWORD** from the **Data Type** drop-down list.

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

- Enter **1** for the **Data:** value in the **DWORD Editor**.

- Click **OK** to close the **DWORD Editor**.

Windows 2000/XP:

Using the MMC Local Policy snap-in as described in Chapter 4 of the *NSA Windows 2000 guide* entitled *"Security Configuration Tool Set:"*

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

- In the right policy window, select the "**Prevent the dial-up password from being saved**" option and set it to **Enabled**. (XP option is "**FSO: Prevent the dial-up password from being saved**")

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 Delete Cached Roaming Profiles

The default Windows NT/2000/XP configuration caches the profiles of users who log on to a network that uses roaming profiles. This feature is provided for system availability reasons such as the user's machine being disconnected from the network or domain controllers not being available. Even though the profile cache is well protected, to implement a secure Windows NT/2000/XP environment this feature should be disabled.

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

Windows NT:

Set the following registry key:

Hive: HKLM

Key: \Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Name: DeleteRoamingCache

Type: REG_DWORD

Value: 1

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

- Navigate down the **Software\Microsoft\Windows NT\CurrentVersion** path, double clicking on each key along the way.

- Select the **Winlogon** key.

- Select **Add Value**… from the **Edit** menu.

- Enter **DeleteRoamingCache** for **Value Name:**

- Select **REG_ DWORD** from the **Data Type:** drop-down list.

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

- Enter **1** for the **Data**: value in the **DWORD Editor**.

- Click **OK** to close the **DWORD Editor**.

Windows 2000/XP:

Using the MMC Local Policy snap-in as described in the Microsoft Windows Security guides:

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

- In the right policy window, select the "**Delete cached copies of roaming profiles**" 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.

4.3.3 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.

Windows 2000/XP:

Using the MMC Local Policy snap-in as described in the Microsoft Windows Security guides:

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

- In the right policy window, select the "**Disable background refresh of Group Policy**" option and set it to **"Disabled"**. (XP option: **"Turn off background refresh of Group Policy"**).

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.

4.3.4 Change Regedit Association

If **Regedit.exe** is associated with registry files, double-clicking those files in Explorer, or Winfile, will cause Regedit to start executing, permitting editing of the registry files. Windows NT/2000/XP sets up this association by default. This association should be removed. Regedit may be safely associated with an application such as Notepad.

Windows NT/2000/XP:

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.

4.3.5 Display Legal Notice for FTP Server Service

If the FTP Server Service is enabled on a platform, the following procedure will configure it to display a required legal notice. *Appendix B* in the *NSA Windows NT Guide* has an example that meets the legal requirements for such warnings.

- *(3.012: CAT II) The SA will ensure that FTP is configured to display a legal notice, if FTP services are enabled.*

Windows NT:

Set the following registry key:

Hive: HKLM

Key: \System\CurrentControlSet\Services\MSFTPSVC\Parameters

Name: GreetingMessage (see *Appendix B* in the *NSA NT Guide*)

Type: REG_MULTI_SZ

Value: *<enter legal notice>*

- Select the **HKEY_LOCAL_MACHINE** on the local machine window.
- Navigate down the **System\CurrentControlSet\Services** path, double clicking on each key along the way.
- Select the **Services** key.
- Select **Add Key**… from the **Edit** menu.
- Enter **MSFTPSVC** for **Key Name:**
- Select the **MSFTPSVC** key.
- Select **Add Key**… from the **Edit** menu.
- Enter **Parameters** for **Key Name:**
- Select the **Parameters** key.
- Select **Add Value**… from the **Edit** menu.
- Enter **GreetingMessage** for **Value Name:**
- Select **REG_ MULTI_SZ** from the **Data Type:** drop down list.
- Click **OK** in the **Add Value** window.
- Enter the ***legal message text*** in the data system in the **MULTI_SZ Editor**.
- Click **OK** to close the **MULTI_SZ Editor**.

4.3.6 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.

Windows NT/2000/XP:

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.

4.3.7 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.

Windows NT/2000/XP:

Set the following registry key:

Hive: HKLM

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

Name: ExtensionAgents

Value: "value containing (Software/Microsoft\LANNanagerMIB2Agent\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 the *NSA Windows Guides,* and *Appendix A* of the applicable Checklists. 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:

Windows NT/2000/XP:

REGISTRY KEY	***USER GROUPS***	***RECOMMENDED PERMISSIONS***
\MACHINE\Software\Classes\Regfile\ Shell\Open\Command	Authenticated 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 NT are listed in the *NSA Windows NT Guide*, Chapter 6, page 42, and for Windows 2000/XP are listed in the *NSA Windows Guides*.

NOTE: The recommended setting (value of 3 or 5) for the LMCompatibilityLevel Registry key as listed in the NSA NT Guide may cause trust failures while trying to map shared resources in another domain. In a mixed-mode Windows 2000, domain, similar problems can occur when NT v4.0 boxes are attached to the domain. At a minimum it is required 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** (zero) or no key is not acceptable.*

Example:

Windows NT:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\LMCompatibilityLevel REG_DWORD, 0x1

Refer to the Microsoft article, *"How to Disable LM Authentication on Windows NT,"* at the following URL:

http://support.microsoft.com/support/kb/articles/Q147/7/06.asp

Windows 2000/XP:

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 "**Send LM & NTLM – use NTLMv2 session security if negotiated"**. (XP option "**Network Security: LAN Manager authentication level"**).

NOTE: In Windows NT domains, set it to Send LM & NTLM – use NTLMv2 session security if negotiated.

In a Windows 2000 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

The required setting for the AutoAdminLogon Registry key as listed in the *NSA NT Guide*, Chapter 13, page 77, incorrectly shows the value type as REG_DWORD. All the Microsoft documentation says that the value type should be a REG_SZ. The requirement is for this value to be a REG_SZ.

NOTE: Since the current level of both Windows NT and Windows 2000/XP appear to make this specific setting effective with either type, if the required value is set, a value type of REG_DWORD will still be a finding, but the severity code will be reduced to a CAT II. This is still a finding because future service packs or releases may cause this error to make the setting ineffective.

Example:

Windows NT:

Configure or delete the following key:

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

Delete the following value if it exists:

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

Windows 2000/XP:

Using the MMC Local Policy snap-in as described in the Microsoft Windows Security guides:

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

- In the right policy window, select the "**Permit administrator automatic logon"** option and set it to "**Disabled**". (XP option: "**Recovery Console: Allow automatic administrative logon").**

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.

4.5.3 Password Policy

The setting for password length as listed in the *NSA Windows Guides* is a minimum of **12** characters. However, the policy is to permit a minimum password length of eight characters.

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

- *(4.013: CAT II) The SA will ensure that the minimum password length is set to eight characters.*

- *(2.009: CAT II) The SA will ensure that each password is 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 will ensure that the complex password filter, EnPasFlt.dll, which was developed by NSA, is installed and active on each machine. Using the PPE product for complex password checking and a password length of seven characters also meets the requirement.*

NOTE: Under Windows 2000/XP, 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 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.

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 but policy will exist to require these to be changed annually.

- *(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.*

NOTE: Under Windows 2000/XP, 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 System Administrator can correct this problem by entering the following on a command line:

Net user <*account_name*> /passwordreq:yes

4.5.4 Unsigned Driver Installation Behavior (Windows 2000/XP)

The setting for the Security Option "**Unsigned driver installation behavior**" (Windows 2000), or "**Devices: Unsigned driver installation behavior**" (Windows XP), is to set it to "**Warn but allow installation**" or "**Do not allow installation**". However, if the system is configured to point to a SUS server, then this setting should be set to "**Silently succeed**" to permit un-attended installation of hot fixes.

This page is intentionally left blank.

5. ACCOUNT POLICIES AND USER RIGHTS

5.1 User Rights

The recommendations specified in the *NSA Windows Guides* 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 NT 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*."

- *(4.016: CAT II) The SA will ensure that in Windows NT, the built-in Guest account, Everyone group, Guests group, and Domain Guests group do not have the right to "log on locally."*

- *(4.025: CAT I) The SA will ensure that in Windows 2000/XP, the built-in Guest account, Guests group, and Domain Guests group (XP – include HelpAssistant and Support_388945a0) are assigned the right "deny access to this computer from the network."*

- *(4.026: CAT II) The SA will ensure that in Windows 2000/XP, the built-in Guest account, Guests group, and Domain Guests group (XP – include HelpAssistant and Support_388945a0) are assigned the right "deny log on locally."*

- *(4.009: CAT I) The SA will ensure that individual and group accounts do not have the right to "act as part of the operating system." The IAO will ensure accounts are clearly identified and documented.*

- *(4.009: CAT I) The IAO will ensure that accounts receiving the right "Act as part of the operating system" are be clearly identified and documented with him in accordance with Section 2.7, Local Exceptions, of this document.*

The right to "Act as part of the operating system" can potentially permit an account to bypass the security features of Windows NT. 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. In this situation these restricted rights may be permitted under the following conditions:

- *(4.040: CAT I) The SA will ensure that in Windows XP no one has the right to "allow logon through Terminal Services."*

- *(4.041: CAT II) The SA will ensure that in Windows XP the Everyone group is assigned the right "deny logon through Terminal Services."*

-

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 system 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.*

The following exception to the NSA recommendation for Windows NT is permitted:

Users Rights	Authorized Groups		
	Domain Controllers	**Member Servers**	**Workstations**
Bypass traverse checking	Authenticated Users	Authenticated Users	Authenticated Users

5.2 Windows XP Built-in Accounts

Several new accounts are created as part of the default Windows XP 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.

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

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

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 *NSA 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 NT and Windows 2000 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 NT, 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 system maintenance will not be included in the Auditors group.

- *(1.010: CAT II) The IAO or TASO will ensure the protection of 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 the local policy will preclude those accounts, which are not part of the Auditors group, from changing the file access restrictions on Windows NT/WIN2K/XP Event Logs.*

- *(1.029: CAT II) The IAO and SA will ensure that Event Logs (**APPEVENT.EVT**, **SYSEVENT.EVT**, and **SECEVENT.EVT**) on servers, and workstations performing server functions, 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 and SA will ensure that Full Control access to the Event Logs is given to an Auditors group. The Auditors group will contain 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:

1. Create the following directory: %SystemRoot%\system32\config\EventLogs.
2. Set ACL permissions on this directory. (Auditors – Full Control, System – Full Control, Administrators – Read)
3. Copy the event logs from the \config directory to the new EventLogs directory.
4. Edit the Registry using regedt32.exe.
5. Expand the following key: **HKLM\SYSTEM\CurrentControlSet\Services\EventLog**.
6. Select the Application key.
7. Double-click the "File" value.
8. Change the string value to: %SystemRoot%\system32\config\EventLogs\Appevent.evt.
9. Repeat Steps 5 through 7 for "Security (Secevent.evt)" and "System (Sysevent.evt)."
10. The next time the machine is rebooted it will use the event logs in the EventLogs directory.
11. 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 System Administrator from implementing and managing a viable auditing effort. Every effort should be made to implement auditing according to the *NSA Windows NT/ 2000 guide*s.

- *(4.007: CAT II) The IAO will ensure that all NT, WIN2K servers and NT/WIN2K/XP workstations that share resources (e.g., files, printers, etc.) are configured for auditing according to the NSA Windows Security Guides.*

Log size can be reduced on both workstations and servers 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 DISA Field Security Operations is an acceptable solution.

6.2.1 Audit Log Requirements for Workstations and Servers

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 that the maximum log size for all logs is set to a minimum of 81920 kilobytes.*

Windows NT/2000 workstations that do not share resources should keep sufficient audit information available for supporting the investigation of suspicious events. They should be configured per the *NSA NT Guide/NSA 2000 Guides* instructions with the following exception:

- *(5.001: CAT II) The SA will ensure that on workstations, Event Log Wrapping is set, at a minimum, to "Overwrite Events Older than 30 Days or more."*

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**.

+

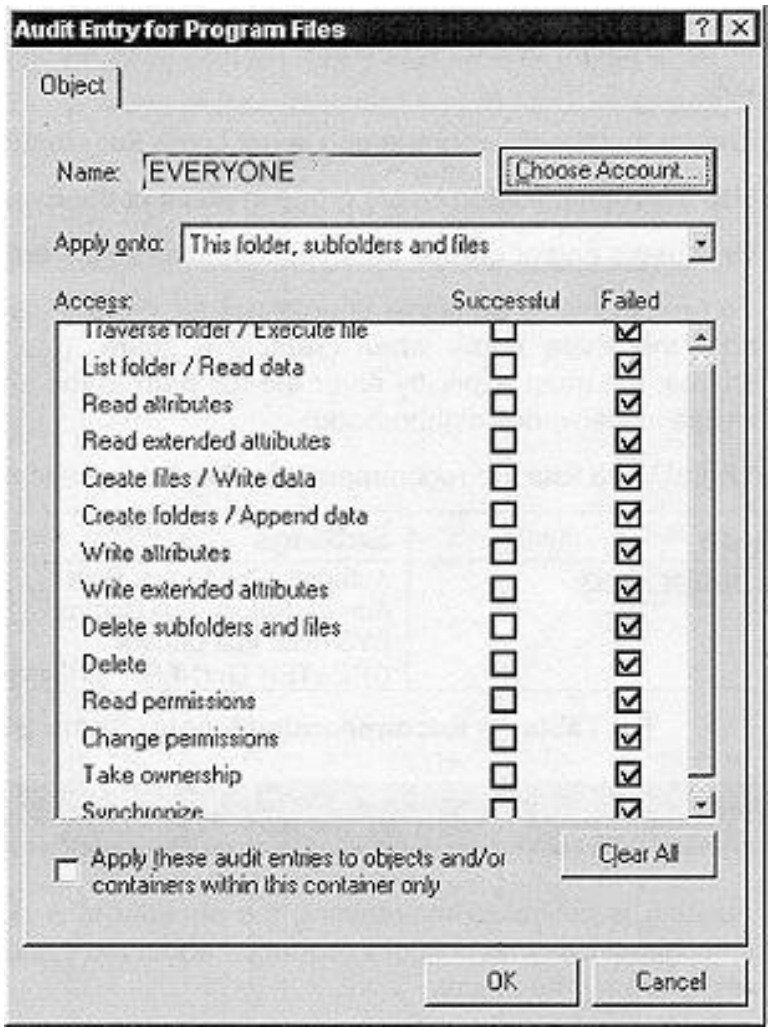
- Reboot the system.

6.4 File Audit Settings

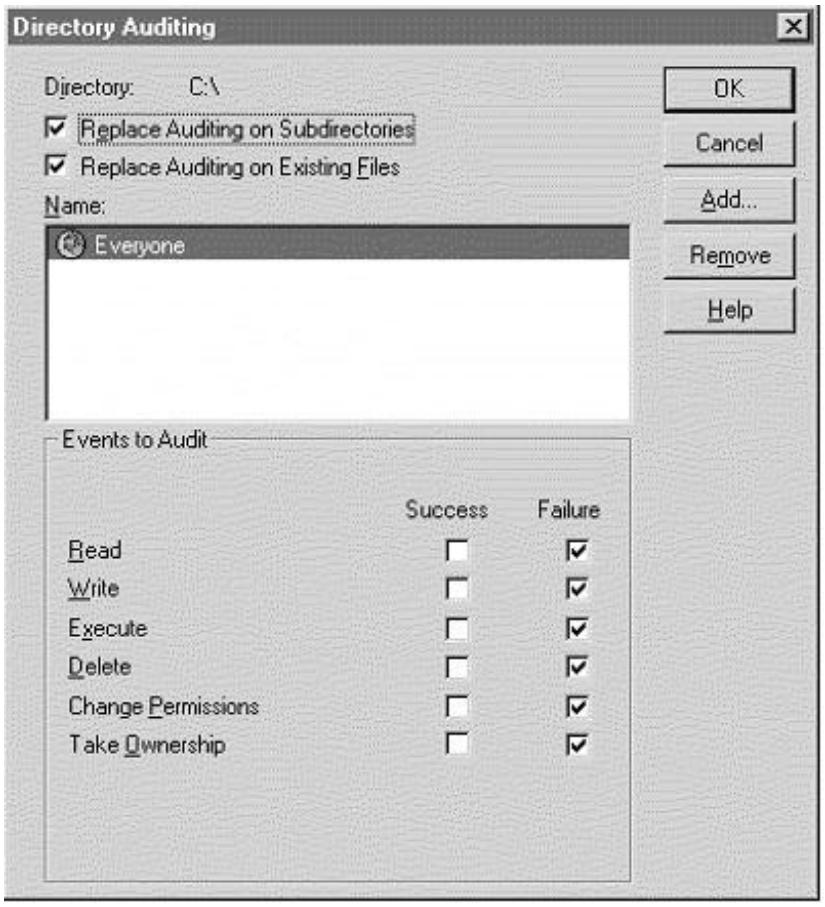
System auditing must be configured using the procedures outlined in the *NSA Windows NT Guide*, the *NSA Windows 2000 Guide: Security Configuration Tool Set*, and NSA Windows XP Guide for any file auditing settings to be effective. File auditing will be set on each local hard drive at the root directory level. Configure File auditing using the procedures found in the *NSA NT Guide,* the *NSA Windows 2000 File and Disk Resources* guide, *and the NSA Windows XP Guide*. One of two audit configuration windows may appear. The Audit Entry for the Program Files figure below, which is the one shown in the *NSA Windows NT Guide*, is the one that

appears if the Microsoft Security Configuration Manager, that came with Service Pack 4, is installed. Windows 2000 uses the same window. It displays the required settings for DOD sites.

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



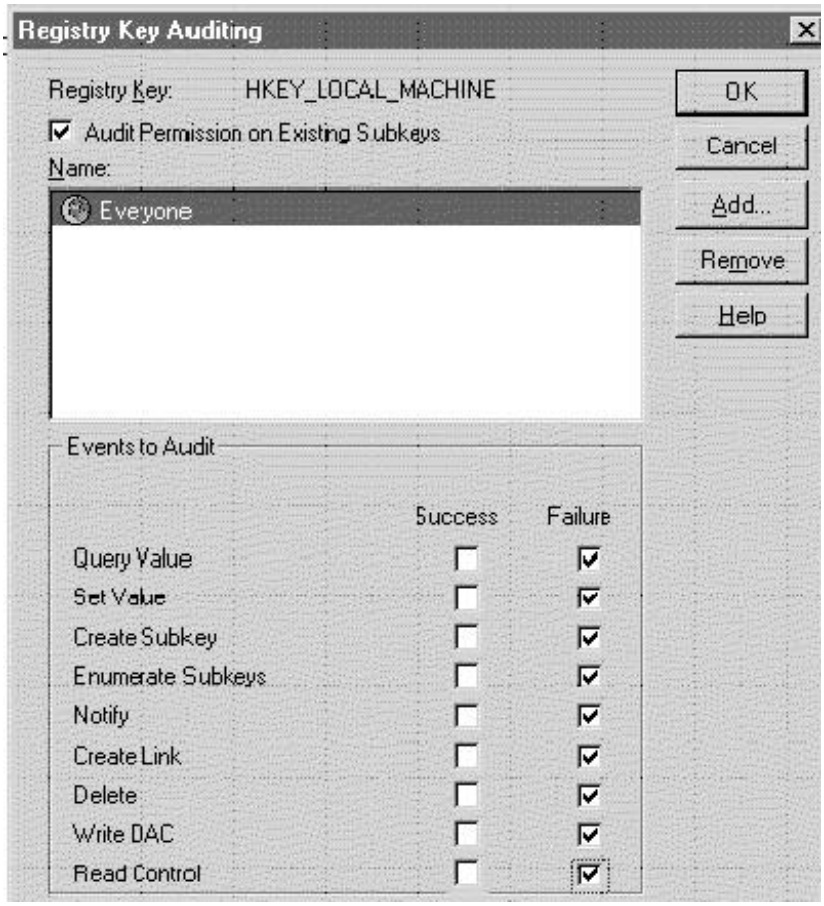
In Windows NT, if the Microsoft Security Configuration Manager has not been installed, or if File Manager is used to configure auditing, then the following Directory Auditing figure will appear. It displays the required settings for DOD sites.



6.5 Registry Audit Settings

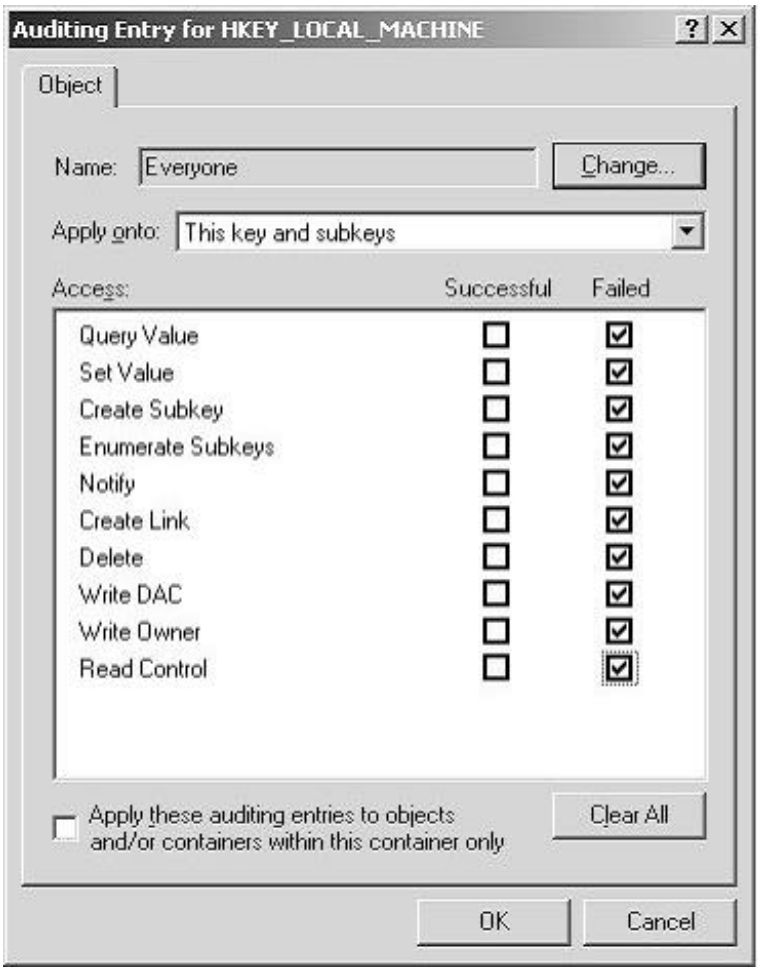
System auditing must be configured using the procedures outlined in the *NSA Windows NT Guide*, the *NSA Windows 2000 Guide: Security Configuration Tool Set*, and the *NSA Windows XP Guide*, for any registry auditing settings to be effective. Configure Registry auditing using the procedures found in the *NSA Windows NT Guide*, Chapter 13, and pages 82–83. (Equivalent procedures are not addressed in the NSA Windows 2000 and Windows XP guides.) Registry auditing will be configured for the ***HKEY_LOCAL_MACHINE*** and ***HKEY_USERS*** hives. The following figure displays the required settings for DOD sites, which differ from the recommended NSA settings, to conform with the CIS Baseline standards:

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



NOTE: Should the site decide to audit the success read control this should not be done on domain controls.

Windows 2000/ XP:



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.

7. GENERAL SECURITY MEASURES

7.1 DOD Physical Security Requirements

No computer will ever be completely secure if people other than the authorized users can physically access it. For maximum security the following applies to servers and workstations that are not physically secure:

- *(1.012: CAT III) The IAO will ensure that servers and workstations 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 7.1.1, Restricting the Boot Process.)*

- *(1.026: CAT III) The SA will ensure that, if the computer does not require network access, 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.

- *(SRC290: CAT II) The IAO will ensure that remote access server cards are not be installed and implemented on any Windows domain controller.*

7.1.1 Restricting the Boot Process

Setting the CMOS:

Set boot options to prevent booting from a floppy disk. 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 floppy disk 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.

7.2 File Security

File permissions will be configured to meet the recommendations in *Appendix F* of the applicable *Checklist*. 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 only the minimum permissions required for applications to function efficiently. The Everyone group will be replaced with the Authenticated Users group (Users group in Windows 2000/XP).

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.).*

7.2.1 Mobile USB Disk Devices (Windows 2000/XP)

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 is recommended that the data be encrypted using an encryption routine that meets DOD encryption standards. The Windows Encrypted File System, Secret Agent, and WinZip version 9.0, are a few products available that can encrypt files and folders. Use of the Windows Encrypted File system, while effective, limits portability of files to systems that support it, and requires that the certificate used to encrypt the files, be on the system where the files are decrypted.

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 IAO will ensure that sites have a clearly defined local policy on the use of Mobile USB Disk devices.*

- *(2.017: CAT II) The IAO will ensure that Mobile USB Disk Devices are formatted with the NTFS file system.*

- *(2.017: CAT II) The IAO will ensure that Mobile USB Disk Devices have file ACLs and Auditing configured in accordance with DOD requirements.*

7.3 Logging Off or Locking the Server/Workstation

Users should either log off or lock the server/workstation 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 that systems are configured to automatically lock with a password-protected screen saver after inactivity of no more than 15 minutes. Five minutes is recommended.*

NOTE: Some terminals require continuous displays, such as network management terminals or Terminal Servers, and are exempt from this requirement. There are screen savers that can continue to show the terminal display and lock the desktop. It is recommended that a screen saver of this type be used if possible.

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.

7.3.1 Configuring Default User Screensaver Options

In an environment where roaming profiles are not used, every user logging on to an Windows 2000 machine for the first time has a profile built for that user using the default user profile stored in the **%Systemroot%\Profile** directory. The default profile can be configured to apply the password-protected screen saver requirements.

- *(3.006: CAT II) The SA will ensure that the default user screensaver options are 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 **Regedt32**. When it opens, open up the **Hkey_Users** window and select the 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 **%systemroot%\Profiles\Default User** directory as **Ntuser.dat**.

3. When **Regedt32** asks for a key name, give it a name the user recognizes. **Regedt32** will import the hive and attach it under the root key under the *hive name* specified.

4. Select the new hive key, and use the **Security>Permissions** menu item to add **Authenticated 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 **Regedt32** 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.

7.4 Installed Services

Windows 2000 Services typically run under the local System Account, which generally has more 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. When possible, the SA should configure services to run under local accounts with the minimum permissions and rights needed to perform their task.

Windows XP has two new service accounts, Network Service and Local Service, which replace the Local System account as service accounts for certain services. The Local Service account has complete privileges on the local system. The Network Service has limited privileges on the local system.

- *(5.068: CAT II) The SA will remove or disable unneeded or unknown services.*

- *(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, at a minimum.*

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

7.4.1 Automatic Updates Service (Windows 2000 / XP)

Service Pack 3 for Windows 2000 installs the Automatic Updates Service. This service enables the download and installation of Windows updates. This service will be disabled to prevent users from downloading and installing updates that have not been approved by the site.

- *(5.014: CAT II) The SA will ensure that the Automatic Updates Service is disabled on Windows 2000/XP machines, if they are not configured to obtain updates from the DOD SUS server or a local SUS server that is configured to pull updates from the DOD SUS server.*

7.4.2 Background Intelligent Transfer Service (BITs) (Windows 2000 / XP)

Service Pack 3 for Windows 2000 installs the Background Intelligent Transfer Service. 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. This service will be disabled to prevent users from downloading and installing updates that have not been approved by the site.

- *(5.015: CAT II) The SA will ensure that the Background Intelligent Transfer Service is disabled on Windows 2000/XP machines, if they are not configured to obtain updates from the DOD SUS server or a local SUS server that is configured to pull updates from the DOD SUS server.*

7.4.3 Fast User Switching Service (Windows XP)

In Microsoft Windows XP, if you enable the Fast User Switching feature, multiple user accounts can log on to a computer simultaneously. If the computer is not part of the domain this feature does not apply.

- *(5.062: CAT II) The SA will ensure that the Fast User Switching service is disabled on Windows XP machines.*

7.4.4 NetMeeting Remote Desktop Sharing Service (Windows 2000/XP)

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 IAO and SA will ensure that the policy option for Computer -> Administrative Templates-> Windows Components -> NetMeeting* ***Disable remote Desktop Sharing*** *is* ***Enabled****.*

7.4.5 Print Services for UNIX

Windows NT/ 2000/XP include TCP/IP-based printing. Print Services for UNIX makes the 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.*

7.4.6 RCMD Service

The RCMD Service allows users to execute command line programs from remote hosts. It is distributed as part of the Windows NT and Windows 2000 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.

- *(5.025: CAT II) The SA will ensure that the RCMD is not installed.*

NOTE: Remove the service by typing **instsrv rcmd remove** at the command prompt.

7.4.7 Remote Access Auto Connection Manager Service (Windows 2000/XP)

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.*

7.4.8 Remote Desktop Help Session Manager (Windows XP)

The Remote Desktop Help Session Manager Service manages and controls the Remote Assistance feature within the XP 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 on XP machines.*

7.4.9 Remote Registry Service (Windows 2000 Professional / XP)

The Remote Registry Service allows you to change registry entries for a remote Windows 2000 / XP 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 Remote Registry Service is disabled on Windows 2000 Professional and XP machines.

7.4.10 Remote Shell Service (RSH)

A version of RSH, which ships with the Windows NT and Windows 2000 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 NT/2000 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 ensure the RSH service is not installed*

NOTE: Remove the service by typing **instsrv rshsvc remove** at the command prompt.

7.4.11 RIP Listener Service

Routers to dynamically exchange routing information use the Routing Information Protocol (RIP). RIP routers broadcast their routing tables every 30 seconds by default. The RIP Listener Service will listen for these RIP broadcasts and update the machines route tables. This service is not installed by default.

- *(5.025: CAT II) The SA will ensure the RIP service is not installed.*

NOTE: This service is removed using the Microsoft Service Applet.

7.4.12 Routing and Remote Access Service (Windows 2000/XP)

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.*

7.4.13 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.

7.4.14 Simple Network Management Protocol (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.*

7.4.15 Simple Service Discovery Protocol (SSDP) Service

The Simple Service Discovery Protocol (SSDP) permits discovery of Universal Plug and Play (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.*

7.4.16 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. In Windows NT, the Schedule service can also be reconfigured to execute commands as a user with lower access rights, which may be a good option for some sites. Some virus checking programs may use the schedule service to run periodic scans on the local machine.

- *(5.009: CAT II) The SA will ensure that, 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.*

- *(5.009: CAT II) The SA will ensure that if used, the schedule service is configured to run under a local account. **(NT Only)***

NOTE 1: The local account should be granted the right to "Log on as a service." This account will be unavailable for user use and will be configured with a complex password, which is changed annually.

NOTE 2: Under Windows 2000 and XP the Task Scheduler service must run under the System Account.

NOTE 3: If the account information on the Task Scheduler service is protected (grayed out), then the following procedure can be used to change it. A qualified, experienced SA who is comfortable working with the NT Registry should only do this:

1. Navigate to the following registry key: HKLM\System\CurrentControlSet\Services\Schedule.
2. Write down the setting for the value "Type." It is probably set to Reg_Dword 0x120.
3. Change the value to 0x10.
4. Leave the registry open, and open the Control Panel. Select the Task Scheduler service.
5. Select the Startup button. (The "log on as" area should no longer be grayed out.)
6. Enter the local account information and click **OK**.
7. Return to the registry and restore the "Type" value to the original setting.
8. Close the Registry.
9. Stop and start the Task Scheduler service; it will now be running under the local account you entered.

In Windows 2000/XP 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:
Hide Property Pages settings 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 pages** is **Enabled**.*

Prohibit New Task Creation settings controls the ability to create new tasks using the new task wizard. Administrators are still able to schedule tasks using the **AT.exe** utility. Since Administrators should only schedule tasks, this setting should be **Enabled**.

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

7.4.17 Telnet Servers

Microsoft released a prototype Telnet server on the workstation and server Windows NT 4.0 Resource Kit CD-ROMs. The Telnet service is included in the default installation of Windows 2000. 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 that sites does not deploy a Windows NT/2000 based Telnet server.*

- *(5.010: CAT II) The SA will ensure that Simple TCP/IP services are disabled.*

7.4.18 Terminal Services (XP)

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 an XP machine.*

7.5 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.

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 that an approved anti-virus product is 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 that signature files are 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.

7.6 Plug and Play (Windows 2000\XP)

With Windows 2000/XP, 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.*

7.7 USB Ports (Windows 2000/XP)

Windows 2000 and Windows XP support 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 that USB ports are disabled, if they are not being used.*

7.8 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 NT/2000 registry and Win32® security functions.

- *(V1339: CAT II) The SA will ensure that the default DCOM authorization level is set at* ***connect*** *or above.*
- *(V1338: CAT II) The SA will ensure that access permissions on DCOM objects do not permit non-administrators to create DCOM objects and execute code on the local system.*
- *(V1349: CAT II) The SA will ensure that launch permissions on DCOM objects do not permit non-administrators to launch applications.*
- *(V1347: CAT II) The SA will ensure that Registry keys for DCOM objects are 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.

7.9 IP Forwarding

IP Forwarding is a feature of Windows NT/2000 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.*

7.10 Trusted Domains

Trusts are used by Windows NT/2000 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.

7.11 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 that the Recycle Bin on servers is configured to delete files immediately on delete.*

It is recommended that the same configuration be used on workstations.

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.

7.12 Lightweight Directory Access Protocol (LDAP) - (Windows 2000)

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 2000 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 2000 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 (Windows 2000 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 NSA "Guide to Microsoft Windows 2000 Active Directory" to ensure that the data that LDAP interacts with is adequately protected.

8. APPLICATION SECURITY

8.1 Software Configuration Management Tools

Software configuration management tools provide the System Administrator a way to track and maintain site software on a network-wide basis from a central location. Products such as 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.

8.2.1 Microsoft Zone Internet Games (Windows XP)

The new Internet Games opens a limited connection to the free games section of the MSN Gaming Zone, which is located at www.zone.msn.com. DOD sites should be prevented from accessing these games.

- *(5.021: CAT III) The SA will ensure that the Microsoft Zone Internet Games option is not installed on the system.*

8.2.2 MSN Explorer (Windows XP)

MSN Explorer is automatically installed with Windows XP. MSN Explorer is a feature that connects the user to the free non-subscriber section of the MSN.com Web site. From this default site the user has access to all of the MSN services. The MSN.com Web site is an Internet connectivity service that provides access to a variety of personal-interest information and services, as well as providing a portal to the World Wide Web.

- *(5.022: CAT III) The SA will ensure that MSN Explorer is not installed on the system.*

8.2.3 IIS Components (XP)

Windows XP comes with a version of Internet Information Services (IIS) that can optionally be installed. This feature permits the hosting of a Web site on the Windows XP machine. Web sites should only be hosted on servers that have been designed for that purpose and can be adequately secured.

- *(5.016: CAT I) The IAO will ensure that Internet Information Services (IIS), or any subset of the Internet Information Services is not installed on the system.*

8.3 Application Security – Microsoft Applications

In 2000 and XP 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 (Windows 2000/XP)

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. Only Administrators should make policy changes, 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** is 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 System Administrator 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** is 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 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 (Windows XP)

Terminal Services are a new addition with Windows XP to the workstation line of Windows Operating Systems. They allow multiple users to connect from remote terminals and use the resources of the local machine as if they were physically at the machine. Terminal Services will not be used and additional settings are required to provide an additional level of security.

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 Allow Local Administrators to Customize Permissions

This setting prevents the local Administrator accounts from modifying the permissions in the Terminal Services Configuration tool. Terminal services configuration should be configured by the Domain Administrators, not by someone with local Administrator rights on the system.

- *(5.041: CAT II) The IAO will ensure that the setting **Do not allow local administrators to customize permissions** is set to **Enabled**.*

8.3.2.6 Remote Control Settings

This setting is used to control the rules for remote control of Terminal Services user sessions. Remote control of sessions should not be allowed.

- *(3.066: CAT I) The IAO will ensure that the setting **Remote control settings** is **Enabled** and that the **Options** are set to **No remote control allowed**.*

8.3.2.7 Always Prompt Client for Password upon Connection

This setting, which is located under the **Encryption and Security** section of the Terminal Services configuration option, controls the ability of users to supply passwords automatically as part of their Remote Desktop Connection. Disabling this setting would allow anyone to use the stored credentials in a connection item to connect to the terminal server.

- *(5.042: CAT II) The IAO will ensure that the setting **Always prompt client for passwords upon connection** is set to **Enabled**.*

8.3.2.8 Set Client Connection Encryption Level

This setting, which is located under the **Encryption and Security** section of the Terminal Services configuration option, controls the encryption that is used for the client connection. This setting will vary depending on the clients that are being used. If a homogenous XP environment is in use, it should be set to **high**. Otherwise it should be set to **Client compatible**.

- *(5.043: CAT II) The IAO will ensure that the setting **Set client connection encryption level** is enabled and set to **high** if in a homogenous XP environment or **client compatible** if non-XP terminal services clients are in use.*

8.3.2.9 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**.*

8.3.2.10 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**.*

8.3.2.11 Set Time Limit for Disconnected Sessions

This setting, which is located under the **Sessions** section of the Terminal Services configuration option, controls how long a session will remain open if it is unexpectedly terminated. Such sessions should be terminated as soon as possible.

- *(5.046: CAT II) The IAO will ensure that the setting **Set time limit for disconnected sessions** is set to **Enabled** and that **End a disconnected session** is set to no more than one minute.*

8.3.2.12 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.*

8.3.2.13 Allow Reconnection from Original Client Only

This setting, which is located under the **Sessions** section of the Terminal Services configuration option, controls whether a different client may be used to resume a disconnected session. Only the original client should be able to resume a session to help prevent **session hijacking**.

- *(5.048: CAT II) The IAO will ensure that the setting **Allow reconnection from original client only** is set to **Enabled**.*

8.3.2.14 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 2000/XP)

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 System Administrators. 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 XP)

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**.*

8.4 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, Windows NT/2000/XP, Tandem, etc.) and can use multiple protocols (TCP, UDP, 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 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 NT/2000/XP, 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 that 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 the 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 that the access control permissions on the MQSeries directory, sub-directories, and files is set in accordance with Appendix A of the Windows NT and Windows 2000 SRR Checklists.*

- *(8.004: CAT II) The SA will ensure that MQSeries services are configured to run under a **local account**, not the system account.*

- *(8.005: CAT II) The SA will ensure that 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 that 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 that the MCAUSER attribute on MQSeries Clients contains a non-blank value or point to a security exit.*

NOTE: 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 NT, Windows 2000, and Windows XP operating systems 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 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.*

9. DISASTER RECOVERY

9.1 Uninterruptible Power Supply (UPS)

An 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 NT/2000 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 the *DISA Computing Services Security Handbook, Section 3.11, Information Operations Condition (INFOCON).*

This page is intentionally left blank.

APPENDIX A. 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

Desktop Application STIG

Network Infrastructure STIG

Web Server STIG

Commercial and Other Publications

Microsoft Corporation White Paper, *Securing Windows NT Installation*, 23 October 1997.

Robichaux, Paul, *Managing the Windows NT Registry, April 1998,* O'Reilly and Associates, Inc.

Thomas, Steven B, *Windows NT 4.0 Registry - A Professional Reference,* 1998, McGraw-Hill.

Web Sites

DISA –	http://www.disa.mil
DISA Datahouse –	https://datahouse.disa.mil
DISA Information Assurance– (Guides, tools)	https://iase.disa.mil http://iase.disa.smil.mil (SIPRNet)
DOD-CERT –	http://www.cert.mil
DOD SUS Servers –	http://dodsus.csd.disa.mil and http://dodsus.csd.disa.smil.mil
DOD SUS Server Information –	http://dodsus.csd.disa.mil/client/install.htm http://dodsus.csd.disa.smil.mil/client/install.htm
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
Patch Listings –	https://patches.csd.disa.mil (NIPRNet) https://patches.csd.disa.smil.mil (SIPRNet)
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 B. INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

B.1 WINDOWS NT SERVER OR WORKSTATION INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

This appendix lists all IAVM bulletins applicable to a **Windows NT server** or **workstation**, including applications that may be installed. This list is complete as of February 2004. Refer to the current NT checklist for the most up-to-date listing.

IAVM BULLETINS FOR WINDOWS NT 4.0

DOD-CERT IAVM Alerts (IAVM) – NT

IAVM 2002-A-SNMP-003 – Multiple Simple Network Management Protocol Vulnerabilities
IAVM 2002-A-SNMP-005 – Multiple Simple Network Management Protocol Vulnerabilities
IAVM 2003-A-0005v2 Microsoft Ntdll.dll Buffer Overflow Vulnerability
IAVM 2003-A-0007 – Buffer Overflow Windows Locator Service
IAVM 2003-A-0012 Microsoft RPCSS DCOM Interface Buffer Overflow Vulnerability
IAVM 2003-A-0017, Microsoft Messenger Service Buffer Overrun Vulnerability

DOD-CERT IAVM Bulletins (IAVB) -NT

IAVM 2002-B-0008 – Microsoft X.509 Certificate Validation Vulnerability
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 - NT

IAVM 1999-T-0011 - Fragmented Internet Group Management Protocol (IGMP)
IAVM 1999-T-0017 - Microsoft TCP Initial Sequence Number Randomness Vulnerability
IAVM 2000-T-0001 - Microsoft NT 4.0 Spoofed LPC Post Request Vulnerability
IAVM 2000-T-0002 - Microsoft “Registry Permissions” Vulnerability
IAVM 2000-T-0005 IP - Fragment Assembly Denial of Service Vulnerability
IAVM 2002-T-0007 Unchecked buffer in MS Multiple UNC Provider Vulnerability
IAVM 2003-T-0008 Microsoft RPC Endpoint Mapper Vulnerability

DOD-CERT IAVM Technical Advisories - Terminal Server

IAVM 1999-T-0005, Denial of Service Attack Against Windows NT Terminal Server

IAVM BULLETINS FOR SERVICES AND APPLICATIONS

DOD-CERT IAVM Alerts – Microsoft Applications

IAVM 2001-A-0012 – Malformed Excel or Powerpoint Document can bypass Macro security
IAVM 2002-A-0005 – Microsoft Data Access Component (MDAC) Buffer Overrun Vulnerability
IAVM 2003-A-0001 – Multiple Vulnerabilities with Microsoft SQL Server
IAVM 2003-A-0016, Microsoft Exchange Server Buffer Overflow Vulnerability

DOD-CERT IAVM Bulletins – Microsoft Applications

IAVM 2002-B-0002, Microsoft Exchange Server 2000 – Malformed Attribute Vulnerability
IAVM 2003-B-0002 – Multiple Vulnerabilities in MS Virtual Machine Java DB

DOD-CERT IAVM Technical Advisories - Microsoft Applications

IAVM 1999-T-0004, Microsoft Exchange Server (Encapsulated SMTP Address) Vulnerability
IAVM 1999-T-0007 - Microsoft Jet/ODBC Technical Advisory
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 2001-T-0013 – Malformed Excel or PowerPoint document can bypass Macro security
IAVM 2002-T-0001 – Multiple Vulnerabilities with Microsoft SQL Server
IAVM 2003-T-0013, Flaw in ISAPI Extension
IAVM 2003-T-0019, Microsoft WordPerfect Converter Buffer Overrun Vulnerability
IAVM 2003-T-0021, MS Visual Basic for Applications Document Handling Buffer Overrun Vulnerability

DOD-CERT IAVM Alerts (IAVM) – Web Servers

IAVM 1999-0004 - Malformed FTP List Request (IIS)
IAVM 1999-A-0009 - Netscape Enterprise and FastTrack Web Server Vulnerability
IAVM 1999-A-0010 - Microsoft Internet Information Server (IIS) Data Access Components Vulnerability
IAVM 2000-A-0001 - Cross-Site Scripting Vulnerability (IIS)
IAVM 2001-A-0007 - iPlanet Web Servers Expose Sensitive Data via Buffer Overflow
IAVM 2002-A-0002 – Multiple Vulnerabilities in Microsoft IIS
IAVM 2002-A-0003 – Apache Web Server Chunk Handling Vulnerability

DOD-CERT IAVM Bulletins (IAVB) – Web Servers

IAVM 1999-B-0001 - Cold Fusion Application Server Vulnerabilities

DOD-CERT IAVM Technical Advisories – Web Servers

IAVM 1999-T-0003 - Microsoft Internet Information Server (IIS) Data Access Components
IAVM 1999-T-0006 - Microsoft IIS Malformed HTTP Request Header
IAVM 1999-T-0015 - Domain Resolution and FTP Download Vulnerabilities (IIS 4.0 only)
IAVM 2000-T-0003 - Link View Server-Side Component Vulnerability (IIS)
IAVM 2002-T-0013 - MS IIS Heaped Overrun in HTR Chunked Encoding Vulnerability
IAVM 2003-T-0003 - Multiple Vulnerabilities in Apache Web Server
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 2000-A-0001 - Cross-Site Scripting Vulnerability
IAVM 2001-A-0004 - Incorrect MIME Header Can Cause IE to Execute E-mail Attachment
IAVM 2003-A-0014, Multiple Vulnerabilities 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 1999-T-0008 - Microsoft Virtual Machine Sandbox Vulnerability (IE)
IAVM 1999-T-0013 - Microsoft Internet Explorer (ActiveX) Vulnerability
IAVM 2000-T-0006 - Frame Domain Verification, Unauthorized Cookie Access and Malformed Component Attribute Vulnerabilities (IE)
IAVM 2000-T-0010.1 - Microsoft “IE Script” and “Office 2000 HTML Script”
IAVM 2000-T-0011 - Malformed E-mail Header Vulnerability
IAVM 2000-T-0013 - Scriplet Rendering Patches (IE)
IAVM 2001-T-0001 – Outlook, Outlook Express Vcard Handler contains unchecked buffer
IAVM 2002-T-0003 - VBScript in IE allows Web pages to read local files

DOD-CERT IAVM Alerts (IAVA) - Other Applications

IAVM 2002-A-SNMP-006 – Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications.
IAVM 2003-A-0008, Multiple Overflow Vulnerabilities in Snort

DOD-CERT IAVM Bulletins (IAVB) - Other Applications

IAVM 2000-B-0001, Bind NXT Buffer Overflow
IAVM 2001-B-0002 – Vulnerability in HP OpenView and IBM NetView
IAVM 2001-B-0003 – ISS RealSecure %U Encoding Intrusion Detection System Bypass Vulnerability

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-0004 – Multiple Vulnerabilities in Oracle 9i Application Server
IAVM 2003-T-0006 – Vulnerabilities in McAfee ePolicy Orchestrator Agent
IAVM 2003-T-0018, Real Networks Universal Server Vulnerability
IAVM 2004-T-0001, DameWare Buffer Overflow Vulnerability

B.2 WINDOWS 2000 - INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

This appendix lists all IAVM bulletins applicable to a **Windows 2000 server or workstation**, as of the effective date of this document, including applications that may be installed. This list is complete as of February 2004. Refer to the current WIN2K checklist for the most up-to-date listing.

IAVM BULLETINS FOR WINDOWS 2000

DOD-CERT IAVM Alerts - WINOS

IAVM 2002-A-SNMP-003 – Multiple Simple Network Management Protocol Vulnerabilities
IAVM 2002-A-SNMP-005 – Multiple Simple Network Management Protocol Vulnerabilities
IAVM 2003-A-0005v2 – Buffer Overflow Vulnerabilities in WIN2K
IAVM 2003-A-0007 – Buffer Overflow Windows Locator Service
IAVM 2003-A-0012 Microsoft RPCSS DCOM Interface Buffer Overflow Vulnerability
IAVM 2003-A-0017, Microsoft Messenger Service Buffer Overrun Vulnerability
IAVM 2003-A-0018, Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability

DOD-CERT IAVM Bulletins - WINOS

IAVM 2000-B-0007, HyperTerminal Buffer Overflow Vulnerability
IAVM 2002-B-0008 - Microsoft X.509 Certificate Validation Vulnerability
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 - WINOS

IAVM 2000-T-0005, IP Fragment Assembly Denial of Service Vulnerability
IAVM 2002-T-0007 – Unchecked buffer in MS UNC Provider Vulnerability
IAVM 2003-T-0008 - Microsoft RPC Endpoint Mapper Vulnerability

IAVM BULLETINS FOR SERVICES AND APPLICATIONS

DOD-CERT IAVM Alerts – Microsoft Applications

IAVM 2001-A-0012 – Malformed Excel or PowerPoint document can bypass Macro Security
IAVM 2002-A-0005 – Microsoft Data Access Component (MDAC) Buffer Overrun Vulnerability
IAVM 2003-A-0001 – Multiple Vulnerabilities with Microsoft SQL Server
IAVM 2003-A-0001v1, Multiple Vulnerabilities with Microsoft SQL Server
IAVM 2003-A-0016, Microsoft Exchange Server Buffer Overflow Vulnerability

DOD-CERT IAVM Bulletins – Microsoft Applications

IAVM 2002-B-0002 - Microsoft Exchange Server 2000 – Malformed Attribute Vulnerability
IAVM 2002-B-0007 – Multiple Vulnerabilities in MCMS 2001
IAVM 2003-B-0002 - Multiple Vulnerabilities in MS Virtual Machine Java DB

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-0010.1 - 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 2001-T-0013 – Malformed Excel or PowerPoint document can bypass Macro security
IAVM 2002-T-0001 – Multiple Vulnerabilities with Microsoft SQL Server
IAVM 2003-T-0014, Media Service Logging ISAPI buffer overflow
IAVM 2003-T-0019, Microsoft WordPerfect Converter Buffer Overrun Vulnerability
IAVM 2003-T-0021, MS Visual Basic for Applications Document Handling Buffer Overrun Vulnerability
IAVM 2003-T-0023, MS FrontPage Server Extensions Remote Debug Buffer Overrun Vulnerability

DOD-CERT IAVM Alerts (IAVM) – Web Servers

IAVM 2000-A-0001 - Cross-Site Scripting Vulnerability (IIS)
IAVM 2001-A-0007 - iPlanet Web Servers Expose Sensitive Data via Buffer Overflow
IAVM 2002-A-0002 – Multiple Vulnerabilities in Microsoft IIS
IAVM 2002-A-0003 – Apache Web Server Chunk Handling Vulnerability

DOD-CERT IAVM Bulletins (IAVB) – Web Servers

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories – Web Servers

IAVM 2002-T-0013 - MS IIS Heaped Overrun in HTR Chunked Encoding Vulnerability
IAVM 2003-T-0003 - Multiple Vulnerabilities in Apache Web Server
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 2001-A-0004 - Incorrect MIME Header Can Cause IE to Execute E-mail Attachment
IAVM 2003-A-0014, Multiple Vulnerabilities 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 2000-T-0006 - Frame Domain Verification, Unauthorized Cookie Access, and Malformed Component Attribute Vulnerabilities (IE)
IAVM 2000-T-0010.1 - Microsoft "IE Script" and "Office 2000 HTML Script"
IAVM 2000-T-0011 - Malformed E-mail Header Vulnerability
IAVM 2000-T-0013 - Scriplet Rendering Patches (IE)
IAVM 2001-T-0001 - Outlook, Outlook Express Vcard Handler Unchecked Buffer (IE)
IAVM 2002-T-0003 - VBScript in IE allows Web pages to read local files.

DOD-CERT IAVM Alerts (IAVM) - Other Applications

IAVM 2002-A-SNMP-006 – Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications.
IAVM 2003-A-0008, Multiple Overflow Vulnerabilities in Snort

DOD-CERT IAVM Bulletins (IAVB) - Other Applications

IAVM 2000-B-0008, Bind 8.2.2-P6 Denial of Service Vulnerabilities
IAVM 2001-B-0002 – Vulnerability in HP OpenView and IBM Tivoli NetView
IAVM 2001-B-0003 – ISS RealSecure %U Encoding intrusion detection system bypass vulnerability

OD-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-0004 - Multiple Vulnerabilities in Oracle 9i Application Server
IAVM 2003-T-0006 - Vulnerabilities in McAfee ePolicy Orchestrator Agent
IAVM 2003-T-0018, Real Networks Universal Server Vulnerability
IAVM 2004-T-0001, DameWare Buffer Overflow Vulnerability

B.3 WINDOWS XP - INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE

This appendix lists all IAVM bulletins applicable to a **Windows XP workstation**, as of the effective date of this document, including applications that may be installed. This list is complete as of February 2004. Refer to the current WINXP checklist for the most up-to-date listing.

IAVM BULLETINS FOR WINDOWS XP

DOD-CERT IAVM Alerts (WinOS)

IAVM 2003-A-0007 – Buffer Overflow Windows Locator Service
IAVM 2003-A-0005v2 Microsoft Ntdll.dll Buffer Overflow Vulnerability
IAVM 2003-A-0012 Microsoft RPCSS DCOM Interface Buffer Overflow Vulnerability
IAVM 2003-A-0017, Microsoft Messenger Service Buffer Overrun Vulnerability
IAVM 2003-A-0018, Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability

DOD-CERT IAVM Bulletins (WinOS)

IAVM 2002-B-0008 – Microsoft X.509 Certificate Validation Vulnerability
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 (WinOS)

IAVM 2002-T-0007 – Unchecked buffer in MS UNC Provider Vulnerability
IAVM 2003-T-0008 – Microsoft RPC Endpoint Mapper Vulnerability

IAVM BULLETINS FOR SERVICES AND APPLICATIONS

DOD-CERT IAVM Alerts – Microsoft Applications

IAVM 2001-A-0012 – Malformed Excel or PowerPoint document can bypass Macro Security

DOD-CERT IAVM Bulletins – Microsoft Applications

IAVM 2003-B-0002 – Multiple Vulnerabilities in MS Virtual Machine Java DB

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-0010.1 - 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 2001-T-0013 – Malformed Excel or PowerPoint document can bypass Macro security
IAVM 2003-T-0019, Microsoft WordPerfect Converter Buffer Overrun Vulnerability
IAVM 2003-T-0021, MS Visual Basic for Applications Document Handling Buffer Overrun Vulnerability
IAVM 2003-T-0023, MS FrontPage Server Extensions Remote Debug Buffer Overrun Vulnerability

DOD-CERT IAVM Alerts (IAVM) – Web Browsers

IAVM 2003-A-0014, Multiple Vulnerabilities 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

There are currently no IAVMs in this category.

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
IAVM 2003-T-0018, Real Networks Universal Server Vulnerability
IAVM 2004-T-0001, DameWare Buffer Overflow Vulnerability

APPENDIX E. SECURITY CONFIGURATION TOOLS

Introduction

With Windows NT 4.0, Service Pack 4, Microsoft introduced the **Security Configuration Manager (SCM)** for configuring security settings on an NT machine. With Windows 2000/XP, the same functionality is provided by the Microsoft Management Console, using the Security Configuration Toolset (SCT) snap-in.

This utility consists of an interactive, graphical piece that allows an administrator to define or modify a security configuration. This file can be used interactively, to either analyze or configure the security settings. It also includes a batch utility, consisting of the **Secedit.exe** program, which can be used to analyze or configure a machine without the need to have the interactive piece installed.

DISA Field Security Operations has incorporated the batch SCM/SCT utility and its related files, along with configuration files for both workstations and servers. This script is capable of configuring the preponderance of security settings needed for a Windows NT/2000 machine to conform to the C2 recommendations of the *NSA Window Guides* and the this *Addendum*. The SCM/SCT utility is available from the web sites mentioned in *Section 1.9, STIG Distribution*.

NOTE 1: In Windows NT, after the machine has been configured using the SCM tool, the views used normally for verifying that File/Registry auditing and Registry ACL permissions may not reflect the current configuration. Using the SCM tool will be necessary to verify and configure system settings.

NOTE 2: The DumpSEC utility can be used to verify registry audit settings. DumpSEC is available for download from SomarSoft, Inc. (http://www.systemtools.com/somarsoft).

Running the Batch Utilities (Windows NT/2000)

NOTE: The configuration files on the configuration tool for Windows 2000 can also be imported into the Security Configuration and Analysis MMC snap-in and used to configure security using that tool. They can also be imported into the various Windows 2000 policies. However, some additional manual configuration will need to be done, which is normally done by the batch script.

The SCM Batch Utility:

1. Log on to Windows with Administrator rights.

2. Insert the disk with the **FSOscm.exe** program. (**WIN2KSCM.exe** for Windows 2000)

3. Select **Start**, **Run**, and enter **A:\FSOscm.exe**.

4. Follow the prompts to direct the configuration process.

   (On a Windows NT machine, during the configuration process the following warning message will appear twice:

   (This is normal and nothing is modified that should not be).

5. When complete, remove the disk and reboot the machine prior to making any other changes.

NOTES:

1. This process renames the Administrator account to **xadministrator**. This can be changed to meet the user's requirements. The password is not affected.

2. Running the SCM utility adds a significant amount of information to the registry. Prior to running the SCM, check the registry size and increase it if it is close to the maximum size specified. The amount of space required varies depending on the number of applications that have been loaded on the machine.

3. If users receive messages while trying to log on indicating that they cannot access their profiles, increasing the size of the registry will generally correct the problem.

WARNING: These settings have been found to be effective in a typical workstation and server environment. However, application requirements may dictate changes to this "typical" configuration. This process should be thoroughly tested in a lab environment to ensure the functionality of applications, prior to installing it in a production environment.

Divergence from Recommended Settings

Based on experience testing the Security Configuration Manager at Field Security Operations and at other organizations, the following changes were made to the *NSA NT Guide* and *NSA Windows 2000 Guides* recommendations:

On All Windows NT/2000 Machines:

1. To permit the proper creation of Internet Explorer profiles for new users, the following permissions on registry keys are set by SCM as follows:

   - HKLM\SOFTWARE\Microsoft\Windows (QSCEN D R) **(NT only)**
   - HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall (QSCEN R) **(NT only)**
   - HKU\.Default (QSCEN R)

2. Audit log settings are different for servers and workstations.

On Windows NT/2000 Servers:

Auditing for registry keys are set as shown in section 6.5.

(Successful *reads* (**R**) are not audited on servers, since this will rapidly fill up the event log.)

Recommended Settings Not Configured by SCM

The following are not configured by this process and have to be done manually:

1. The SCM will not set the screen saver settings for accounts that already have profiles on the machine. These settings will have to be done manually using the procedure outlined in *Section 7.3.1, Configuring Default User Screensaver Options,* of the this *Addendum*.

2. Add an Auditors group and assign permissions to that group on the Event Log files.

3. On servers and workstations, the following user right will have to be set manually to remove the Administrators group and add an Auditors group:

   Manage auditing and security log

4. On servers, several user rights settings will have to be edited and set manually. This is to accommodate applications that require rights that would normally not be granted to individual accounts. These rights are as follows:

   - Act as part of the operating system
   - Log on as a batch job
   - Log on locally
   - Log on as a service

5. Set a CMOS password.

6. Convert a file system to NTFS, if applicable.

7. Remove a \DOS directory.

8. Set share permissions.

9. Install approved virus protection software.

10. Properly configure the FTP service when it is required or disable it.

11. Set file permissions on partitions, other than the **%SYSTEMDRIVE%** and **%SYSTEMROOT%**.

12. Add, disable, or remove accounts.

Modifying the SCM Configuration Files

The configuration files included with the Batch SCM/SCT disk were developed to conform closely to the security recommendations of the *NSA NT* and *Windows 2000 Guides* and this *Addendum*. These have been tested at Field Security Operations and used by several DOD organizations. However, operational needs or application requirements may require that an organization deviate from the recommended settings. A knowledgeable System Administrator can modify the configuration files. The configuration files should not be modified directly, but through the use of the interactive, graphical SCM/SCT interfaces.

For Windows NT the installation and use of the SCM graphical tool is explained in great detail in the *NSA NT Guide*.

On Windows 2000, the Security Configuration and Analysis MMC snap-in is an integral part of the installation for each machine. Its use is detailed in the NSA Windows 2000 Group Policy guide entitled *"Security Configuration Tool Set."*

When the interactive SCM utility is installed, it creates a set of Registry keys that determines which registry settings appear in the tool's **Local Policies/Security Options** graphical window to permit modification. Field Security Operations has added additional keys to this list. To be able to modify these additional settings, it will be necessary to overlay the default registry keys with the updated set.

Windows NT:

The updated list of keys is included on the SCM batch disk as **regkey.dat**. To load these updated keys, do the following:

1. Open the Registry using **Regedt32.exe .***.

2. Navigate to **MACHINE/Software/Microsoft/Windows NT/CurrentVersion/SeCEdit/Reg Values**.

3. Highlight the **Reg Values** key.

4. On the Menu bar, select **Registry/Save** key and save the current list of keys.

5. On the Menu bar, select **Registry/Restore** and point to the **regkey.dat** file on the SCM batch disk.

6. Reply **Yes** to the warning message that the current keys will be overlaid.

7. Close **Regedt32**.

The additional registry settings will now appear in the SCM graphical window.

* ***Only an experienced System Administrator should make changes to the NT Registry. The Registry should always be backed up prior to making changes.***

Windows 2000:

Use the procedure to load the modified Security Options file, as detailed earlier in this document in *Section 4, Securing the Registry and Windows 2000/XP Policies.*

APPENDIX F. ADDITIONAL CIS BASELINE SETTINGS (Windows 2000)

This appendix contains excerpts from the CIS Windows 2000 Operating System Level 2 Benchmark, Consensus Baseline Security Settings.

The FSO Gold Disks for Windows 2000 Professional, Server, and XP and the older Window 2000 Security configuration tools configure these additional settings. These settings have been determined to have a minimal impact on the functioning of most Windows 2000 systems, yet will provide an increased level of security. This is not to say that there will always be no impact. Be sure to note any warnings present on the various configuration settings listed in this appendix.

While the CIS document shows the registry keys involved in the various security settings, The FSO Windows 2000 Configuration tools come with a replacement security options file (Sceregvl.inf), that when loaded, will permit these settings to be modified using the Security Configuration Tool Set (**SCT**). See the applicable Checklists, for instructions on loading the new options file.

The SCT Security Options Headings will also be listed for each recommended setting listed below.

The following paragraphs describe individual security settings that can be applied in a variety of ways – using REGEDIT.EXE, REGEDT32.EXE, Local Group Policy, or Domain Group Policy, FSO Configuration tool, or FSO Gold Disks. For more information on applying changes directly to a Windows 2000 registry, or through Group Policies, please consult the Microsoft TechNet Internet site at http://www.microsoft.com/technet.

Some other helpful registry information is available at:

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q256986 and,
http://www.microsoft.com/technet/prodtechnol/winntas/tips/winntmag/inreg.asp.

WARNING: Editing the registry can make a system unbootable and unusable if done improperly. If you are not familiar with editing the registry, please take a few minutes and follow the links to Microsoft's TechNet resources, and learn about some of the precautions you should take before editing the registry.

F.1. Suppress Dr. Watson Crash Dumps:

HKLM\Software\Microsoft\DrWatson\CreateCrashDump (REG_DWORD) 0

(SCT) CIS: Allow Dr. Watson Crash Dumps – set to "disabled"

Dr. Watson is one of Microsoft's utilities that handle errors in applications. If an application produces an error that Dr. Watson can manage, it will dump the contents of memory for that application to a file for future analysis.

In the process of writing the contents of memory to disk, it is entirely possible that password information could be written to disk as well, and later exploited. Set this value to zero to prevent Dr. Watson from writing crash dumps to disk.

- *(5.071: CAT III) The SA will ensure that the option "**CIS: Allow Dr. Watson Crash Dumps"** is set to **"disabled."***

F.2. Disable Automatic Execution of the System Debugger:

HKLM\Software\Microsoft\Windows NT\CurrentVersion\AEDebug\Auto (REG_DWORD) 0

(SCT) CIS: Automatic Execution of the System Debugger – set to "disabled"

If an application is executed in non-privileged memory, and the system debugger is started, it is possible for that application to execute code in privileged memory space. Set this value to zero to prevent the system debugger from executing automatically.

- *(5.072: CAT III) The SA will ensure that the option "**CIS: Automatic Execution of the System Debugger**" is set to "**disabled**."*

F.3. Disable autoplay for the current user:

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun (REG_DWORD) 255

Although it is convenient for applications to automatically run when Windows Explorer opens up, it can also cause applications to be executed against the wishes of an administrative user, and exploiting that privilege. Set this value to 255 to prevent any type of drive from automatically launching an application from Windows Explorer.

NOTE: Due to the inability to manage registry entries for each local user via Security Templates, this setting is recommended, but not required or measured.

F.4. Disable autoplay for new users by default:

HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\ NoDriveTypeAutoRun (REG_DWORD) 255

(SCT) CIS: Disable Media Autoplay (HKU-.default hive) - set to "Disable autoplay on all drive types"

Although it is convenient for applications to automatically run when Windows Explorer opens up, it can also cause applications to be executed against the wishes of an administrative user, and exploiting that privilege. Set this value to 255 to prevent any type of drive from automatically launching an application from Windows Explorer.

- *(3.090: CAT III) The SA will ensure that the option "CIS: Disable Media Autoplay (HKU-.default hive)" is set to "Disable autoplay on all drive types."*

F.5. Disable automatic reboots after a Blue Screen of Death:

HKLM\System\CurrentControlSet\Control\CrashControl\AutoReboot (REG_DWORD) 0

(SCT) CIS: Reboot the system after a crash – set to "Disabled."

If someone manages to get enough control of your computer that they can plant an application there, the next step is to force your computer to restart to register that app. One easy way to accomplish this task is to programmatically force an error that causes the computer to crash, or "Blue Screen" which will reboot the machine by default. Set this Value to zero to prevent this behavior from happening, and at least alert the user that something is wrong.

- *(5.073: CAT III) The SA will ensure that the option "CIS: Reboot the system after a crash" is set to "Disabled."*

F.6. Remove administrative shares on workstation (Professional):

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareWks (REG_DWORD) 0

(SCT) CIS: Automatically create system shares – set to "Disabled."

Every Windows NT/2000 computer automatically has "Administrative Shares" installed by default. These are restricted to use by Administrators, but they expose each volume root, and the %systemroot% folder to the network as Admin$, C$, etc. These make remote administration convenient, but they also present a risk if someone manages to guess the password to an administrative account.

WARNING: If you use administrative shares on your network for remote backups, antivirus support, or general remote administration, this

will break your applications. Please ask your software vendors to design around this requirement in future versions of their applications.

If possible, the SA should ensure that the option "***CIS: Automatically create system shares***" is set to "**disabled**".

F.7. Enable IPSec to protect Kerberos RSVP Traffic:

HKLM\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt (REG_DWORD) 1

(SCT) CIS: Enable IPSEC security for Kerberos RSVP Traffic – set to "Enabled."

When Kerberos authentication information is transferred between domain controllers, or between domain controllers and member servers or workstations, it is not secured by default. Even when IPSec is used to encrypt that traffic, the Kerberos information is considered "exempt." Set this value to 1 to ensure that all traffic, including Kerberos information, is protected by IPSec.

- *(3.091: CAT II) The SA will ensure that the option "**CIS: Enable IPSEC security for Kerberos RSVP Traffic**" is set to "**enabled**."*

F.8. Do not announce this computer to domain master browsers:

HKLM\System\CurrentControlSet\Services\Lanmanserver\Parameters\Hidden (REG_DWORD) 1

(SCT) CIS: Hide computer name from other domain computers – set to "Enabled."

If the Computer Browser service is disabled, or if this computer is not part of a domain, this setting has no effect. Otherwise, it will prevent the computer from announcing itself to the browser services of other computers, and only act as a "listener" on domain browse lists.

WARNING: This setting will remove your computer from the list of available computers in your domain in Network Neighborhood. Disabling the Computer Browser service should already do this, but this setting will perform the same function.

- *(5.085: CAT III) The SA will ensure that the option "**CIS: Hide computer name from other domain computers**" is set to "**enabled**."*

APPENDIX G. QUICK START CHECKLIST

Use this checklist as step-by-step guidance to comply with STIG requirements when installing a new server or workstation. The FSO Windows NT/2000/XP SRR Checklists, this Addendum, and NSA Windows Guides should be referred to in performing the installation.

For Windows 2000 and Windows XP, many of the procedures listed here can be easily and accurately accomplished using the FSO Gold Disk tool that has been developed for installing and configuring the operating system and specific applications to the current required security levels. Steps that are included in the Gold Disk process are identified with the annotation (Gold Disk). Follow the Gold Disk User guide for the specific configuration for detailed instructions on using the tool.

NOTE: The asterisk "*" next to a requirement denotes a manual process.

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 compliant.
- ☐ Remove any modems installed.
- ☐ Assemble the installation software, current Service Pack(s), and Hot Fix(s). (Gold Disk)
  - ❑ Current approved service pack
  - ❑ Check for additional hot fixes issued.
- ☐ Obtain Norton Anti-Virus or McAfee Virus Shield software and the most current signature file. (Gold Disk)
- ☐ For servers that will have additional functionality, ensure the applicable application software, service pack(s), and hot fix(s) are obtained (e.g., IIS, SQL Server, Terminal Server, etc.).
- ☐ Obtain all IAVM bulletin information for Windows NT /2000/XP and applicable applications. (Gold Disk)

Installation:

Follow these steps to ensure STIG compliance when installing a Windows NT 4.0 / 2000 Server or Workstation / Windows XP Workstation:

- ☐ The new Server (DC or standalone) or Workstation is **not connected** to the network until after configured to STIG compliance.
  - In Windows NT, when installing a BDC, ensure that the PDC is fully STIG compliant prior to installation of the BDC. After an NT Server is configured as a BDC, immediately disconnect it from the network, until the STIG requirements are configured.
- ☐ Install Windows according to manufacturer instructions and site configuration requirements. (Gold Disk)
  - Format or convert the system's hard drive to the NTFS file system.
- ☐ Install current service pack and applicable hot fixes. (Gold Disk)
- ☐ Install Norton Anti-Virus or McAfee Virus Shield software and the most current signature file. (Gold Disk)
- ☐ Create the ERDs.
  - Performing a full backup may be advisable at this point if additional applications are to be installed.
- ☐ Run the FSO SCM/SCT configuration scripts (Gold Disk), and apply manual settings.

NOTE: Some System Administrators have reported problems with using the SCM configuration scripts to configure servers when additional applications are to be installed. It may be advisable to install applications first, and then run the SCM configuration scripts.

OR

Configure the machine manually as listed below. Reference the *NSA Windows Guides*, this *Addendum*, and/or the *Windows NT/2000/XP Checklists, Section 5, Configure User Accounts.* Use the SCM or SCT snap-in. A few settings that cannot be set using these tools are marked with an asterisk (*****).

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. (Gold Disk)

- Maximum password age
- Minimum password age
- Minimum password length
- Password uniqueness
- Account lockout
- Bad logon attempts
- Bad logon counter reset
- Lockout duration
- 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 the DOS directory. (Gold Disk)
- ☐ Remove the OS2 and POSIX files. (Gold Disk)
- ☐ *****Copy the ENPASFLT.DLL to %root%\System32 directory. (Gold Disk)
- ☐ Configure the Registry. (Gold Disk)
- ☐ Set the file and directory permissions (access control list). (Gold Disk)
  - ❑ System files
  - ❑ Event logs
- ☐ Set the registry key permissions (access control list). (Gold Disk)
- ☐ Set the appropriate printer share permissions for locally installed printers.
- ☐ Configure installed services.
  - ❑ Remove Remote Shell services.
  - ❑ Disable Scheduler/Task Scheduler services. (Gold Disk)
  - ❑ Disable Simple TCP/IP services.
  - ❑ Disable Telnet services. (Gold Disk)
  - ❑ Remove Fingerd services.
  - ❑ Remove RCMD services.
  - ❑ Disable SNMP services if not required. (Gold Disk)

If a workstation does not share resources on the network:

- Disable Computer Browser service.
- Disable Server service (optional).

☐ 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. (Gold Disk)

☐ Set Event log settings. (Gold Disk)

- Retention settings (server, workstation)
- Log size settings (server, workstation)

☐ Enable Auditing (Gold Disk)

- Enable auditing.
- Set the auditing configuration.
- Set file and directory auditing.
- Set registry auditing.

☐ *****Create User Accounts, if applicable.

☐ *****For NT, install and configure a Software Configuration Management tool.

☐ *****Install and configure an intrusion detection product (all servers).

☐ *****Install and configure MQSeries, if applicable.

☐ *****Perform a sample SRR. (Gold Disk)

- Refer to the *NSA Guides* and this *Addendum*.
- Fix any findings.

Prior to connecting to the network, ensure the following:

☐ Register with VMS.

- System Administrators
- Servers

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

APPENDIX H. LIST OF ACRONYMS

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