ADDENDUM

TO THE

NSA GUIDE TO SECURING MICROSOFT WINDOWS NT NETWORKS

AND

NSA GUIDES TO SECURING WINDOWS 2000

Version 3, Release 1

26 November 2002

DISA
FIELD SECURITY OPERATIONS

This page is intentionally left blank.

TABLE OF CONTENTS

SUMMARY OF CHANGES....vii

1 INTRODUCTION....1
1.1 Background....1
1.2 Purpose....2
1.3 Scope....2
1.4 Authority....3
1.5 Writing Conventions....3
1.6 DISA Information Assurance Vulnerability Management (IAVM) Program/Vulnerability Compliance Tracking System (VCTS) Process....4
1.7 Extensions....4
1.8 STIG Distribution....5
1.9 Document Revisions....5

2 SECURITY ADMINISTRATION....7
2.1 Gold Standard....7
2.2 Security Controls....8
2.3 Patch Control....9
2.4 DISA Form 41, Controlled Access to Machines, Files, and Functions....10
2.5 Administrative Tools....10
2.6 Local Exceptions....11

3 SECURING THE WINDOWS NT/WIN2K OPERATING SYSTEM....13
3.1 Permitted Operating Systems....13

4 SECURING THE REGISTRY AND WIN2K POLICIES....15
4.1 NT/WIN2K Registry Access Policy....15
4.2 WIN2K Active Directory/Group Policy Access Policy....15
4.3 Registry Settings....16
4.3.1 Disable the Option to Save the Password in Dial-up Networking....16
4.3.2 Delete Cached Roaming Profiles....17
4.3.3 Change Regedit Association....19
4.3.4 Display Legal Notice for FTP Server Service (Windows NT)....20
4.3.5 Altered DCOM RunAs Value....21
4.3.6 Restrict NetBIOS Information through SNMP....22
4.4 Access Control for Specific Registry Keys....22
4.5 Recommended Settings Variations....23
4.5.1 LMCompatibilityLevel Registry Key....23
4.5.2 AutoAdminLogon Registry Key....24
4.5.3 Password Policy....25

5 ACCOUNT POLICIES AND USER RIGHTS....27

6 AUDITING....29

6.1 Audit Log Management....29
6.1.1 Evaluating Audit Trails and Log Files....29
6.1.2 Protecting Logs....29
6.2 Audit Log Requirements....30
6.2.1 Audit Log Requirements for Workstations....31
6.3 Audit Failure Procedures....31
6.4 File Audit Settings....32
6.5 Registry Audit Settings....34

7 GENERAL SECURITY MEASURES....37
7.1 DISA Physical Security Requirements....37
7.1.1 Restricting the Boot Process....37
7.2 File Security....38
7.3 Logging Off or Locking the Server/Workstation....38
7.3.1 Configuring Default User Screensaver Options....39
7.4 Installed Services....40
7.4.1 Remote Shell Service (RSH)....40
7.4.2 Windows Task Scheduler Service....40
7.4.3 Server Service....41
7.4.4 Telnet Servers....41
7.4.5 Finger Service....42
7.4.6 RCMD Service....42
7.4.7 SNMP Service....42
7.4.8 Remote Registry Service (Windows 2000 Professional)....42
7.4.9 Automatic Updates Service (Windows 2000)....42
7.4.10 Background Intelligent Transfer Service (BITs) (Windows 2000)....43
7.5 Virus Protection....43
7.6 Distributed Component Object Model (DCOM)....44
7.7 IP Forwarding....44
7.8 Trusted Domains....44
7.9 Recycle Bin....45
7.10 Lightweight Directory Access Protocol (LDAP) - (WIN2K)....45

8 APPLICATION SECURITY....47
8.1 Software Configuration Management Tools....47
8.2 Removing Unneeded Applications....47
8.3 MQSeries....48
8.4 WebSphere Application Server Security....49

9 DISASTER RECOVERY....51
9.1 Uninterruptible Power Supply (UPS)....51
9.2 Domain Backups....51

APPENDIX A. RELATED PUBLICATIONS....53

APPENDIX B. SECURITY CONFIGURATION TOOLS....57

APPENDIX C. WINDOWS NT - INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE..... 63

APPENDIX D. WINDOWS 2000 - INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) COMPLIANCE..... 69

APPENDIX E. QUICK START CHECKLIST..... 73

APPENDIX F. GLOSSARY OF TERMS..... 79

This page is intentionally left blank.

SUMMARY OF CHANGES

September 2002:

- General: Reformatted the document to consolidate or remove several sections and revised section numbering.
- Revised *Section 1, Introduction*. Removed unneeded information revised to conform to a common STIG format.
- Removed *Section 2.1, Required Documentation, Waivers, and Exemptions*. Consolidated with *Section 1.8, STIG Distribution.*
- Added new *Section 2.1, Gold Standard.*
- Revised *Section 2.2, Security Controls*. Added the frequency for baseline reviews. Added NIAP certification as an alternate option to vendor integrity statements.
- Revised *Section 2.3, Patch Control*. Added a bullet requiring the installation of the latest OS and Application service packs.
- Removed *Section 2.3.1, Recovering from a System Compromise.*
- Removed *Section 2.4, Notification Identification, and Eradication.*
- Removed *Section 2.5, Vulnerability Correction.*
- Removed *Section 2.6, Recovery.*
- Added new *Section 2.6, Local Exceptions.*
- Removed *Section 2.5, Department of Defense Computer Emergency Response Team (DOD CERT)*. Incorporated in Section 1.6
- Removed *Section 2.14, Information Operations Condition (INFOCON).*
- Revised *Section 4.1, NT/WIN2K Registry Access Policy*. Reworded the note about maintenance of an ERD.
- Revised *Section 4.5.1, LMCompatabilityLevel Registry Key*. Added a note about settings in a mixed NT/WIN2K environment.
- Removed *Section 4.3.2, Users must log on to change password.*
- Removed *Section 4.3.3, DontDisplayLastUserName Registry Key.*

- Added *Section 4.5.2, AutoAdminLogon Registry Key.*
- Revised *Section 4.5.3, Password Policy.* Added a note about DISANET's use of PPE. Added a requirement related to Application accounts.
- Revised *Section 6.2.1, Audit Log Requirements for Workstations*. Changed the minimum log size to 80 megabytes.
- Added *Section 6.3, Audit Failure Procedures.*
- Revised *Section 6.4, File Audit Settings*. Removed the requirement for auditing successes to be consistent with the Gold Standard. Audit all failures.
- Revised *Section 6.5, Registry Audit Settings*. Removed the requirement for auditing successes to be consistent with the Gold Standard. Audit all failures.
- Revised *Section 7.1.1, Restricting the boot process.* Limited the boot password requirement to servers.
- Added *Section 7.2, File Security*
- Revised *Section 7.3, Logging off or Locking the Server/Workstation.* Added a note giving an exception to servers requiring continual displays.
- Revised *Section 7.4, Installed Services.* Added requirement for Secure Shell for any remote service access.
- Added *Section 7.4.3, Server Service.*
- Added *Section 7.4.8, Remote Registry Service (WIN2K Professional).*
- Added *Section 7.4.9, Automatic Updates Service (WIN2K).*
- Added *Section 7.4.10, Background Intelligent Transfer Service (BITs) (WIN2K).*
- Revised *Section 7.5, Virus Protection.* Set the maximum age for signature files to 14 days or less. Eliminated duplication of the *Desktop Application STIG.*
- Removed old *Section 7.5, Intelligent External Devices.*
- Added *Section 7.10, LDAP (WIN2K).*
- Added *Section 8.2, Removing Unused Applications.*

- Added *Section 8.4, WebSphere.*

- Revised *Appendix A, Related Publications.*

- Moved *Appendix B, Glossary of Terms*, to the end of the document and changed the letter designations for the other appendices. (*Appendix B* is now *Appendix F, Glossary of Terms*.)

- Revised *Appendix C, Windows NT IAVMs*.

- Revised *Appendix D, Windows 2000 IAVMs*.

- Revised *Appendix E, Quick Start Checklist.*

December 2001:

- Revised *Section 2.3, Security Controls*. Modified the requirement for baseline checking to apply to Servers and critical workstations.

- Revised *Section 2.12.2, Protecting Logs*. Added a note about configuring the event logs so permissions will be changed when they are cleared.

- Revised *Section 4.3.4, Password Policy*. Added a note about setting user accounts in WIN2K to show that passwords are required.

- Revised *Section 6.1, Audit Log Requirements*. Reworded the last paragraph to reflect minimum requirements for maintaining the integrity of audit data.

- Revised *Section 7.1.1, Restricting the Boot Process*. Added an exemption for a boot password requirement for Operations machines that are kept in a restricted, physically secured environment.

- Revised *Section 7.3.2, Windows NT/WIN2K Task Scheduler Service*.

- Added a note about changing the Task Scheduler service to run under a local account, when the account maintenance area is protected (grayed out).

November 2001:

- Revised *Section 2.13, Administrative Tools*. Made references to the use of vulnerability checking and intrusion detection tools general in nature rather than recommending a specific product.

- Added *Section 4.3.4, Password Policy*.

- Revised *Section 7.6, Distributed Component Object Model (DCOM).*

- Revised *Section 8.2, MQSeries*.

September 2001:

- Made modifications to add references and unique procedures for Windows 2000 (WIN2K).

- Revised *Section 1.4, Writing Conventions*, for consistency.

- Revised *Section 1.5, Document Distribution*, for consistency.

- Revised *Section 1.6, Related Documentation*, to add a list of *NSA Guides*.

- Updated *Section 2, Security Administration*, to include Security Controls and Recovery Procedures.

- Revised *Section 2.14, Information Operations Condition (INFOCON)*, for consistency.

- Added a new section entitled *Section 4.3, Recommended Settings Variations*.

- Updated *Appendix D, Windows NT – Information Assurance Vulnerability Alert (IAVM) Bulletin Compliance*, which has a current list of IAVM bulletins that apply to NT and installed applications.

- Added *Appendix E, Windows 2000 – Information Assurance Vulnerability Alert (IAVM) Bulletin Compliance*, which has a current list of IAVM bulletins that apply to WIN2K.

December 2000:

- Changes made since the previous release (Version 1, Release 3) are shown in red font throughout this document for ease of identifying the most recent changes in soft copy.

  NOTE: This is no longer the practice due to printer problems with the red font.

- Reworded some requirements as a result of recommendations from the September TIM (Technical Interchange Meeting) review.

- *Section 1.5, Document Distribution* – Corrected the server URL and added the SIPRNet URL.

- *Section 2.3, Security Controls* – Reworded the 3rd italicized bullet regarding Vendor Integrity Statements being requested, either directly or through Field Security Operations, for all commercial software. Added a final paragraph in the section stating that a list of current Vendor Integrity Statements will be published on the DISA Information Assurance web site.

- *Section 2.4, Patch Control* – Added this new section.

- *Section 2.4 – 2.10* – Renumbered these sections.

- *Section 2.5, DOD-CERT* – In the 1st italicized bullet, added a reference to *Appendix D, IAVM Bulletin Compliance*. In the 2nd italicized bullet, added a reference to the ISSO ensuring that all applicable application-specific IAVM Bulletins are responded to and implemented in a timely fashion.

- *Section 2.8.2, Protecting Logs* – Revised the 1st paragraph about setting file access restrictions to limit the viewing and editing of Event Logs. In the 4th italicized bullet, added a reference to the ISSO reviewing Event Logs ***on critical machines*** for unauthorized access.

- *Section 2.9, Administrative Tools* – Added a paragraph at the end of the section to give users a contact for obtaining the latest ESM templates.

- *Section 4, Securing the Registry* – Updated the reference to the *NSA NT Guide*.

- *Section 4.1.4, Display Legal Notice for FTP Server Service* – Updated the reference to the *NSA NT Guide*.

- *Section 6.1, Audit Log Requirements for Workstations* – Moved *Workstation* settings to the new *Section 6.1.1, Audit Log Requirements for Workstations*. Regarding the Audit Server project, the last sentence of *Section 6.1* was changed to add a reference indicating that the project was implemented by DISA Field Security Operations.

- *Section 6.2, File Audit Settings*, and *Section 6.3, Registry Audit Settings* – Updated the references to the *NSA NT Guide*.

- *Section 7.2.1, Configuring Default User Screensaver Options* – Updated the ScreenSaveTimeout detail to "**(in seconds, 900=15 minutes)**". Changed the 2nd sentence in the 6th numbered paragraph to indicate that these settings will now be applied to a new profile when it is created.

- *Section 7.4, Virus Protection* – Updated the download site name. Added the IAVM Bulletin list.

- *Section 7.9, Recycle Bin* – Added an italicized bullet and a paragraph regarding the use of the Recycle Bin on servers and workstations.

- *Section 9.1, Uninterruptible Power Supply (UPS)* – Reworded the only italicized bullet to state that the ISSO or TASO will ensure that each Windows NT ***production*** server is on a UPS.

- *Appendix A, Related Publications* – Updated the list of web sites.

- *Appendix B, Glossary of Terms* – Changed the name of *Appendix B* (was previously *Acronyms and Abbreviations*) to be consistent with other STIGs and Addendums. Added new terms.

- *Appendix C, DISA CIO Standard Computer Configuration Memorandum* – Removed this appendix and replaced it with *Appendix C, Security Configuration Tools*.

- Added a 3rd note under *The SCM Batch Utility* in the new *Appendix C* regarding what users should do if they receive messages while trying to log on indicating that they cannot access their profiles.

- *Appendix D, IAVM Bulletin Compliance* – Added the IAVM Bulletin references and compliance details.

- *Appendix E, Quick Start Checklist* – Added the Quick Start Checklist.

- *Appendix F, Record of Changes* – Moved the *Record of Changes* to the beginning of the document. Removed it as an appendix and changed the title to *Summary of Changes* to be consistent with other STIGs and Addendums. Added the *Document Revision Request* form (as *Appendix F*).

August 2000:

- *Section 6.1, Audit Log Requirements for Workstations* – Added an exclusion to audit log setting requirements for alternative auditing methodologies.

- *Section 7.2, Logging Off or Locking the Server/Workstation* – Added an exception to screen saver requirements for applications running continuous real-time displays.

- *Section 8.1, Software Configuration Management Tools* – Changed the requirement for using SMS to a general requirement for an approved software configuration management tool.

- *Appendix D, Security Configuration Tools* – Modified instructions for updates to the Field Security Operations SCM tool.

May 2000:

- Updated the document to conform to the new *NSA NT Guide*, dated 3 February 2000, by removing several sections that were duplicated in the NSA (National Security Agency) document.

- Added *Appendix D, Security Configuration Tools*.

- Added *Appendix E, Record of Changes*.

This page is intentionally left blank.

1 INTRODUCTION

1.1 Background

This Addendum to the NSA Guide to Securing Microsoft Windows NT Networks (NSA NT Guide) and NSA Guides to Securing Windows 2000 (NSA WIN2K Guides), has been developed to enhance the confidentiality, integrity, and availability of sensitive Defense Information Systems Agency (DISA) Automated Information Systems (AISs) using the Windows NT and Windows 2000 operating system. The guidance presented in this document for Windows 2000 can also be applied, for the most part, to Windows XP Professional, for which NSA is currently developing a guide.

This Addendum is coordinated with the following documents:

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

Department of Defense (DOD) Directive 8500.1, Information Assurance, 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." DISA Instruction 630-230-31 assigns the DISA Principle Director for Operations with the responsibility to develop and maintain Security Technical Implementation Guides (STIGs). These STIGs (or *Addendum*, as appropriate) serve as the security configuration guidelines required by DODD 8500.1. The specific guidance contained in this Addendum will change considerably in the future with the new international standard (Common Criteria for Information Technology Security Evaluation – ISO/IEC 15408) being implemented by the National Information Assurance Partnership (NIAP) and the planned release of DOD Instruction 8500 bb. These issues will be addressed in an upcoming release of this Addendum. This document has been supplemented with additional information concerning specific operating system environments including the Microsoft Windows NT, Windows 2000, and Windows XP operating systems.

1.2 Purpose

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 NT Guide/NSA WIN2K Guides with DISA-specific requirements. This Addendum will assist the following sites in meeting the minimum requirements, standards, controls, and options that must be in place for secure network operations. Each of the following will be referred to hereafter as a **site**:

- Defense Enterprise Computing Centers (DECCs)
- Defense Enterprise Computing Center - Detachments (DECC-Ds)
- Global Network Operations and Security Centers (GNOSCs)
- Network Operations and Security Centers (NOSCs)
- Regional Network Operations and Security Centers (RNOSCs)
- Systems Support Offices (SSOs)
- DOD Components
- Combatant Commanders
- DISA Continuity of Operations and Test Facility (DCTF)
- Other DISA customers

Because customer-driven requirements and site operating environments are so varied, a **cookie-cutter** approach to security is not practical. The Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO), 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 specifies the minimum requirements for securing the Windows NT/Windows 2000 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 ISSO will ensure the system's overall secure operation.

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

1.3 Scope

The requirements set forth in this document will assist SAs, ISSOs, and ISSMs in securing the Windows NT/Windows 2000 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 Authority

The Security Technical Implementation Guides (STIGs) were initially developed to assist the sites in securing their systems against security and infrastructure vulnerabilities. All sites have a vested interest in maintaining system security, as it directly impacts the site's Certification and Accreditation (C&A). Sites are mandated by DISA to have a valid C&A status by the authority derived from *Department of Defense (DOD) Directive 8500.1, Information Assurance, 24 October 2002*, and the *Computer Security Act of 1987, Public Law 100-235, January 1988*. The requirements for accreditation of DISA Information Technology, as described here, are found in *DISAI 630-230-19, DISA Information Systems Security Program, July 1996*.

This process has been extended to Joint Commands seeking to secure their systems against the same vulnerabilities. While there is no mandate for their use at the Joint Commands, the value of the STIGs has been seen by each of the Unified Commands.

1.5 Writing Conventions

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

A reference using "**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 ISSO or System Administrator (SA) must adhere to the instruction as written. Only a VMS (Vulnerability Management System) extension approved by DISA will table this requirement for DISA facilities. The extension will have an expiration date, and does not relieve the ISSO or SA from continuing their efforts to meet 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. All reasonable attempts to meet these recommendations will be made. However, if certain factors limit the implementation of this recommendation (such as customer requirements), written documentation will be maintained explaining the reason why the conditions cannot be met and what alternative implementation strategy is supplementing the instruction.

1.6 DISA Information Assurance Vulnerability Management (IAVM) Program/Vulnerability Compliance Tracking System (VCTS) Process

DISA developed and mandated the Vulnerability Compliance Tracking System (VCTS) to notify its commands, agencies, and organizations of new and potential security vulnerabilities. The VCTS meets the DOD mandate to ensure that information system vulnerability alert notifications are received and acted on by all System Administrators (SAs). It provides a mechanism to ensure that new vulnerabilities are corrected within the specified time period. It provides the means, via the SRRDB (Security Readiness Review Database), for scheduling periodic validations of system status. VCTS and the SRRDB have recently been combined into the Vulnerability Management System (VMS). Users who require access to VMS should contact the Weblog Help Desk at Defense Switched Network (DSN) 570-5690, commercial (717) 267-5690, or e-mail to **weblog@chamb.disa.mil**.

Each site will ensure that all DISA information systems and their SAs register with the VCTS. A DISA information system is a system that is physically located at a DISA site or managed by DISA personnel. The site will be responsible for registering all new systems and all new SAs with the VCTS. The ISSO and ISSM will be responsible for ensuring that all Information Assurance Vulnerability Management (IAVM) notices are responded to and/or implemented. The Field Security Operations SRRDB tracks the site implementation status of all IAVM alerts, bulletins, and technical advisories. The SRRDB can provide SRR review teams with a list of system specific IAVM notices as well as the applicable fixes and patches. The SRR Team will check each system to ensure IAVM compliance. This document includes detailed information on all IAVM notices issued that apply to this technology. Where applicable, these IAVM notices are referenced or included in summary format in this document. Additional details are found in *Appendix C, Windows NT - Information Assurance Vulnerability Management (IAVM) Compliance*, and *Appendix D, Windows 2000 - Information Assurance Vulnerability Management (IAVM) Compliance*.

- *The ISSO will ensure that all DISA critical assets are registered with the VCTS.*

- *System Administrators (SAs) responsible for information systems will be registered with the VCTS. (ISSM)*

- *The ISSO and ISSM, in coordination with the SA, will be responsible for ensuring that all IAVM notices are responded to within the specified time period.*

1.7 Extensions

With the recent migration of the SRRDB into VMS, one of the major changes is that the previous SRR waiver and exemption process has been discontinued. Instead, sites must submit an on-line request for extension for any SRR finding that cannot be fixed and closed within the designated timeframe. This is the same process used by VCTS. The VMS SRRDB extension process for reviews and approvals will be similar as well.

Deviations from the standards will be allowed as long as:

- C2/EAL controls are not jeopardized
- A true business case justifies each deviation
- The security of the site is not adversely affected.

After a Security Readiness Review (SRR), a report of findings will be presented to the organization. If findings cannot be resolved in a timely manner, an extension may be requested. Justification may include operational reasons, technical conflicts, and insufficient funding. An extension request should identify a plan and timetable for resolving the finding(s). Any supplemental security countermeasures should also be addressed.

1.8 STIG Distribution

Compliance with the applicable Security Technical Implementation Guide (STIG) is mandatory for systems residing in a DISA facility and for any system directly administered by DISA. 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 C2 system high level or Evaluated Assurance Level (EAL) 3 level, containing unclassified but sensitive information. In the interest of promoting enhanced security for systems both inside DOD and within the Federal Government's computing environments, DISA encourages any interested DOD activity or party to obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is http://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. The DISA Field Security Operations (FSO) URL is http://guides.ritchie.disa.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a **.mil** or **.gov**. The STIGs are available to users that do not originate from a **.mil** or **.gov** by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to **fso_spt@ritchie.disa.mil**.

1.9 Document Revisions

Revisions to this document should be sent via e-mail to **stig_comments@ritchie.disa.mil**. DISA Field Security Operations will coordinate all change requests with the relevant DISA Field Security Operations organizations, and other DISA organizations as appropriate, before inclusion in this document.

This page is intentionally left blank.

2 SECURITY ADMINISTRATION

This section addresses administrative security requirements that are unique to DISA organizations and are required by DISA 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 box to a production or development network, unless the individual site requires a more secure standard. It was developed by a consortium of government and civilian organizations that included DISA Field Security Operations, NSA, NIST (National Institute of Standards and Technology), CIS (Center for Internet Security), and many others. Settings were chosen with the intent to configure the box 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 work is in progress on baselines for WIN2K Servers and Windows NT.

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

For the purpose of conforming to SRR requirements, DISA organizations will configure systems to meet what it calls a Platinum Standard, which equates to the current requirements in the NSA NT and WIN2K guides and this Addendum.

Field Security Operations will provide three configurations for both NT and WIN2K that will be available for systems (Workstation, Member Server, Domain Controller) for which a Gold Standard has been agreed upon:

- The Gold Standard configuration, developed by the consortium
- The standard DISA FSO configuration, which encompasses the Platinum Standard
- A “Delta” configuration, which can be applied to the Gold Standard to raise it to Platinum level

2.2 Security Controls

Windows NT and WIN2K are operating systems in which the typical OS function and networking are integrated. Windows NT and WIN2K 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 ISSO will ensure a Windows NT/WIN2K workstation or server is configured to provide compliance with the security required by *Department of Defense (DOD) Directive 5200.28* 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:

- *Products will be evaluated for sensitive functions that could compromise NT/WIN2K security, and will implement controls to protect those functions. All security controls implemented will be coordinated with, and approved by, DISA Field Security Operations. (ISSM)*

- *The SA, under the direction of the ISSO, is responsible for creating, checking, and maintaining a current system baseline for all servers and critical workstations. The ISSO is responsible for verifying the system baseline. The ISSM is responsible for setting overall policy for system baseline creation and maintenance.*

- *Sites will 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 SABI (Secret and Below Interoperability) secure guards that have a minimal Operating System (OS) tailored to the specific requirements of the device. (ISSM)*

  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. One of the recommended system baseline utilities is the Axent ESM (Enterprise Security Manager) application used to obtain and check system baselines.

- *Baseline reviews will be done weekly on each critical system. (SA)*

- *The SA should maintain three weeks of baseline product reports and be able to provide them upon request.*

- *All baseline backups will be maintained on write-protected media. (SA)*

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.

- *At a minimum, the operating system ***.exe**, ***.bat**, ***.com**, ***.cmd**, and ***.dll** files will be baselined and compared.*

- *DISA servers will use host-based Intrusion Detection Systems (IDSs) on all systems. (ISSM)*

  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.

- *The ISSO will ensure that all commercial IA software is NIAP certified or that a Vendor Integrity Statement has been requested, either directly or through Field Security Operations.*

  NOTE: *If a specific IA product is not listed with NIAP, but an equivalent product is, then the equivalent must be used.*

DISA Field Security Operations maintains a file of Vendor Integrity Statements. To determine if a Vendor Integrity Statement is on file for a commercial product, contact the Field Security Operations Point-of-Contact (POC) at 717-267-9347 or DSN 570-9347.

A list of current Vendor Integrity Statements is available on the DISA Information Assurance web sites (http://iase.disa.mil or http://iase.disa.smil.mil).

2.3 Patch Control

Maintaining the security of a Windows NT/WIN2K system requires frequent reviews of security bulletins. Many security bulletins mandate the installation of a software patch (**hotfix**) to overcome security vulnerabilities.

SAs and ISSOs should regularly check OS vendor web sites for information on new security patches that are applicable to their site.

- *The ISSO will ensure that the Standard Operating Procedure (SOP) for each system includes the requirement to monitor Department of Defense Computer Emergency Response Team (DOD-CERT) bulletins at http://www.cert.mil. Select the link to the DOD-CERT bulletins.*

- *The ISSO and SA will subscribe to the DOD-CERT/VCTS (Vulnerability Compliance Tracking System) bulletin mailing list. (See Section 1.6, Information Assurance Vulnerability Management (IAVM) Program/Vulnerability Compliance Tracking System (VCTS) Process.)*

- *The ISSO will ensure that software patches are applied and documented.*

- *The ISSO will ensure that the latest OS and Application service packs are applied and documented.*

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

2.4 DISA Form 41, Controlled Access to Machines, Files, and Functions

Access should be requested and granted in writing. For DISA organizations, the vehicle for requesting and granting access and for defining the scope of access is *DISA Form 41*.

- *The ISSO will ensure that **all users** are identified on DISA Form 41 (or the equivalent for non-DISA organizations) to include site staff and SAs that support the systems. The forms should be maintained at the level where access is granted.*

2.5 Administrative Tools

DISA Field Security Operations recommends the use of automated vulnerability and intrusion detection products to assess the vulnerability of the sites' Windows NT/WIN2K operating systems. Microsoft has incorporated several utilities to assist in assessing Windows NT/WIN2K vulnerabilities.

- *For Windows NT, the ISSO or TASO will use the Security Configuration Manager, as described in Chapters 3 through 12 of the NSA NT Guide.*

- *For WIN2K, the ISSO 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."*

2.6 Local Exceptions

If certain factors limit the implementation of **recommended** enhancements (such as customer requirements, or unique application requirements), written documentation will be maintained explaining the reason why the conditions cannot be met and what alternative implementation strategy is supplementing the instruction.

- *The ISSO will maintain a file for each server/workstation that has deviations to security recommendations. The file will document each exception and contain a risk assessment for each deviation that the site Commander has approved. Lack of such documentation will result in findings for non-compliant systems.*

  NOTE: *Exceptions that affect the site as a whole or a significant group of systems can be consolidated into a single file.*

For **mandatory** requirements that cannot be met, only an extension as outlined in *Section 1.7, Extensions,* will suffice.

This page is intentionally left blank.

3 SECURING THE WINDOWS NT/WIN2K 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. The same settings, for the most part, can be configured on a WIN2K system. C2 requirements will be used to evaluate the strength of a Windows NT system. When the evaluation has been completed by NSA, Common Criteria will be used to measure the strength of a WIN2K system.

- *The ISSO will ensure that the system will boot only to STIG compliant operating systems. Exceptions will be approved and documented by the ISSO, where applicable, and each operating system will meet the provisions of the appropriate STIG.*

This page is intentionally left blank

4 SECURING THE REGISTRY AND WIN2K POLICIES

4.1 NT/WIN2K Registry Access Policy

Implementing security measures within the Windows NT/WIN2K 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/WIN2K 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.

- *The ISSO 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. Follow the instructions for* ***Manual Settings*** *in Chapter 13 of the* ***NSA NT Guide*** *and in Chapter 8 of the* ***NSA WIN2K Guide*** *for the "****Security Configuration Tool Set****" in making registry updates.*

4.2 WIN2K 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. It is essential that the Active Directory and Group-level policies are protected from alteration by unauthorized or untrained persons.

- *The ISSO 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.*

- *The ISSO will ensure that security recommendations in the NSA WIN2K 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 WIN2K machines, provision has been made to modify some of these settings through the MMC, using Security Configuration and Analysis, and Policy snap-ins. Follow the general guidance for modifying Security Options in the *NSA WIN2K Guide* for "*Security Configuration Tool Set.*" Explicit instructions for WIN2K machines, when applicable, are provided in the following sections.

The following sections outline recommended additions to the registry changes required by the *NSA Guides.*

> ***NOTE: On WIN2K machines, load the updated Security Options File, following instructions in Section 5.1 of the FSO WIN2K SRR Checklist. This file adds additional NSA 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/WIN2K 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 NT/WIN2K 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.

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**.

WIN2K:

Using the MMC Local Policy snap-in as described in Chapter 4 of the *NSA WIN2K 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**.

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/WIN2K 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/WIN2K environment this feature should be 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**.

WIN2K:

Using the MMC Local Policy snap-in as described in Chapter 4 of the *NSA WIN2K 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 "**Do not allow caching 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 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/WIN2K sets up this association by default. This association should be removed. Regedit may be safely associated with an application such as Notepad.

Windows NT and WIN2K:

Set the following registry key:

Hive: HKLM

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

Name: <No Name>

Type: REG_SZ

Value: notepad.exe "%1"

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

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

- Select the **Command** key.

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

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

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

4.3.4 Display Legal Notice for FTP Server Service (Windows NT)

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 NT Guide* has an example that meets the legal requirements for such warnings. FTP will be 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 box in the **MULTI_SZ Editor**.
- Click **OK** to close the **MULTI_SZ Editor**.

4.3.5 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 and WIN2K:

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.

4.3.6 Restrict NetBIOS Information through SNMP

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

Windows NT and WIN2K:

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 NT Guide, NSA WIN2K Guide: Security Configuration Tool Set,* and *Appendix A* of the *Windows NT* and *Windows 2000 SRR Checklists*. In addition there are other keys that require additional protection.

- *Non-administrators will not be allowed to change the command associations for registry files. (SA)*

Configure the following permissions:

Windows NT and WIN2K:

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 NT Guide*, Chapter 6, page 42, and for WIN2K are listed in the *NSA WIN2K Guide: Security Configuration Tool Set*, Chapter 4, pages 41-42.

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. It is recommended to set the Registry key value to 1, if this problem occurs.*

- *Set the LMCompatibilityLevel registry key 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

WIN2K:

Using the MMC Local Policy snap-in as described in Chapter 4 of the *NSA WIN2K 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 **LAN Manager authentication level** option and set it to **Send LM & NTLM – use NTLMv2 session security if negotiated**.

  NOTE 1: *In NT domains, set it to Send LM & NTLM – use NTLMv2 session security if negotiated.*

  *In a WIN2K 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 recommended setting for the AutoAdminLogon Registry key as listed in the *NSA 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 Field Security Operations requirement is for this value to be a REG_SZ.

NOTE: *Since the current level of both Windows NT and Windows 2000 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 Category 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

WIN2K:

Using the MMC Local Policy snap-in as described in Chapter 4 of the *NSA WIN2K 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 Permit administrator automatic logon option and set it to Disabled.

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

4.5.3 Password Policy

The recommended setting for password length as listed in the *NSA Guide*, Chapter 5, page 30, and the *NSA WIN2K guide* entitled "*Security Configuration Tool Set,"* Chapter 2, page 22, is a minimum of **12** characters. However the DISA Field Security Operations policy is to permit a minimum password length of eight (**8**) characters.

- *Minimum password length will be set to eight (**8**) characters. (SA)*

- *Each password will be composed of at least one of each of the four character types: upper-case, lower-case, numeric, and special characters. (SA)*

- *The complex password filter, EnPasFlt.dll, which was developed by NSA, will be installed and active on each machine.* (DISANET uses the PPE product for complex password checking and a password length of seven (**7**) characters. This product provides enforcement that is at least as secure as the EnPasFlt filter.) *(SA)*

  NOTE: *Under Windows 2000, several user accounts will 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

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.

- *For Application accounts, the ISSM will ensure that there is a local policy in place that requires them to be changed on a yearly basis.*

5 ACCOUNT POLICIES AND USER RIGHTS

The recommendations specified in the *NSA NT Guide/NSA WIN2K Guides* will be followed in assigning user rights. In addition, the SA will ensure that the following requirements are applied:

- *In Windows NT the built-in Guest account, Everyone group, Guests group, and Domain Guests group will not have the right to* ***access this computer from the network****.*

- *In Windows NT, the built-in Guest account, Everyone Group, Guests group, and Domain Guests group will not have the right to* ***log on locally****.*

- *In WIN2K, the built-in Guest account, Guests group, and Domain Guests group will be assigned to the right* ***deny access to this computer from the network****.*

- *In WIN2K, the built-in Guest account, Guests group, and Domain Guests group will be assigned to the right* ***deny log on locally****.*

- *Individual and group accounts will not have the right to* ***act as part of the operating system****.*

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:

- *Accounts receiving this right will be clearly identified and documented with the ISSO in accordance with Section 2.6, Local Exceptions, of this document.*

- *Passwords for these accounts will be the maximum length permitted, will follow the* ***strong password*** *rules, and will be kept in a locked container accessible only by the ISSO and his designated backup.*

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

- *Exceptions to User Rights recommendations for applications will be documented with the ISSO.*

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

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 regular basis to identify security breaches and potential weaknesses in the security structure.

- *The ISSO 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.*

- *The ISSO or TASO will protect Event Logs from unauthorized administrators or users who might change or delete them. All access to Event Logs will be audited, and archived logs will remain under locked control.*

- *Local policy will preclude those accounts, which are not part of the Auditors group, from changing the file access restrictions on Windows NT/WIN2K Event Logs. (ISSM)*

- *Event Logs (**APPEVENT.EVT**, **SYSEVENT.EVT**, and **SECEVENT.EVT**) on servers, and workstations performing server functions, will be 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). (ISSO/SA)*

- *The ISSO will review the Event Logs on critical machines for unauthorized access.*

- *Full Control access to the Event Logs will be 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.) *(ISSO/SA)*

  NOTE: *Under Windows NT, 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 NT Guide* and the *WIN2K guides*.

- *The ISSO will ensure that all NT/WIN2K servers and workstations that share resources (e.g., files, printers, etc.) are configured for auditing according to the* ***NSA NT Guide*** *and the* ***WIN2K 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 **(7)** 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

NT/WIN2K 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 WIN2K Guides* instructions with the following exceptions:

- *The maximum log size for all logs should be set to a minimum of **81920** kilobytes.* (This value has been revised to reflect the Gold Standard (see *Section 2.1*) *(SA)*

- *Event Log Wrapping should be set to **Overwrite Events Older than 30 Days or more**. (SA)*

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 (see NSA WIN2K Guide: Security Configuration Tool Set, Chapter 4, page 49).

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: The CrashOnAuditFail, at this point, will probably be shown as a REG_None: 0x2.

- 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**.

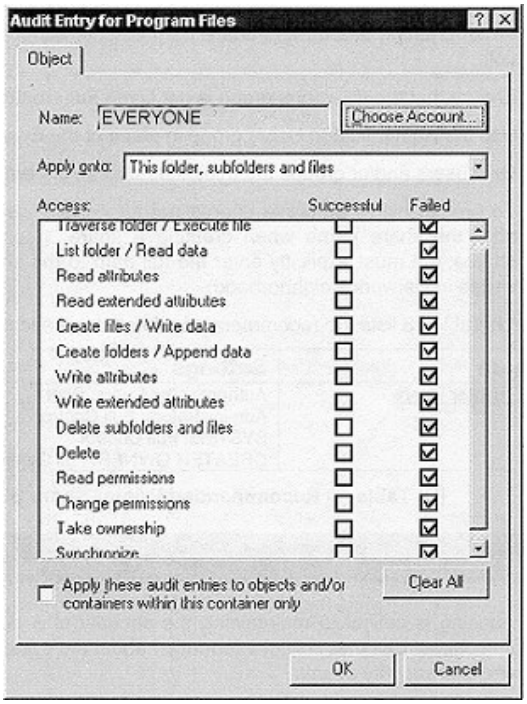
- Enter **CrashOnAuditFail** in the value name field, and select **REG_DWORD** in the data type box. Click **OK**.

- In the Dword editor box enter a value of **1**. Click **OK**.

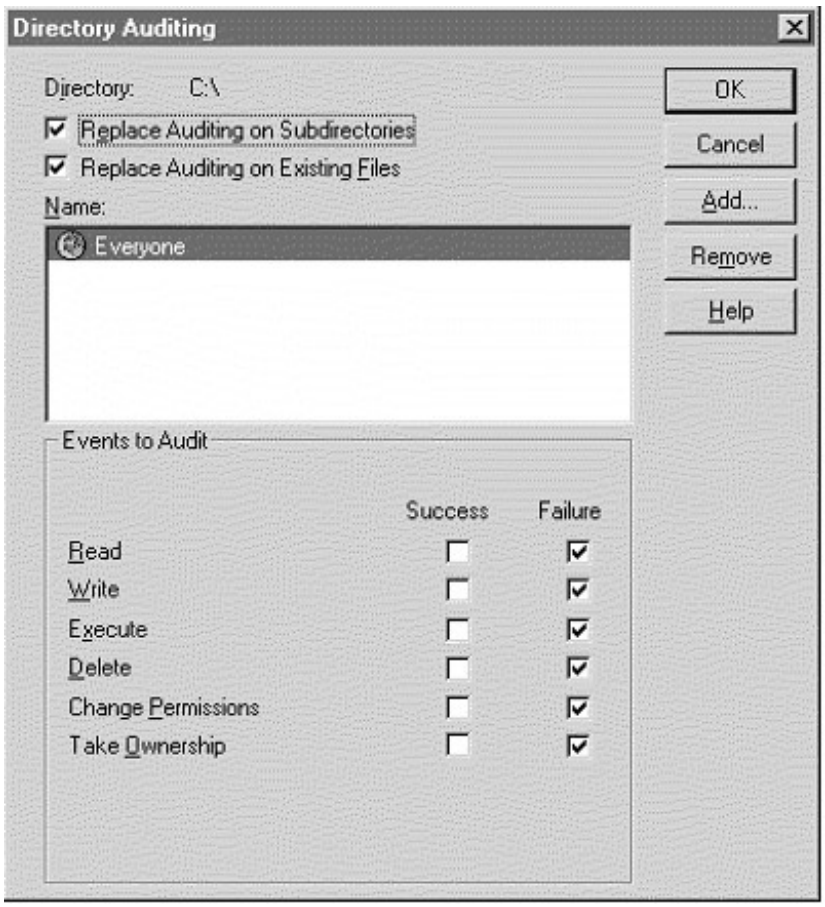
- Reboot the system.

6.4 File Audit Settings

System auditing must be configured using the procedures outlined in the *NSA NT Guide,* Chapter 6, pages 33-34, and the *NSA WIN2K Guide: Security Configuration Tool Set,* Chapter 4, pages 27-28, 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*, Chapter 13, pages 81–82, and the *NSA WIN2K File and Disk Resources* guide, Chapter 3, pages 14-16. 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 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 DISA sites.

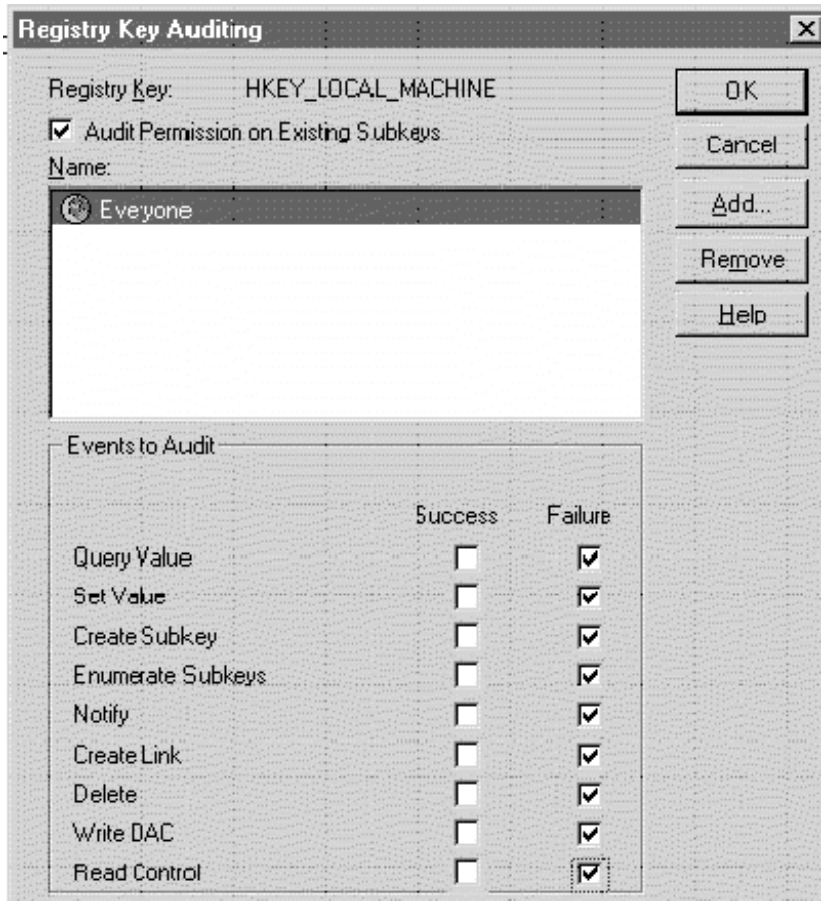


In Windows NT, if the Microsoft Security Configuration Manager has not been installed, or if File Manager is used to configure auditing, then the following Directory Auditing figure will appear. It displays the required settings for DISA sites.



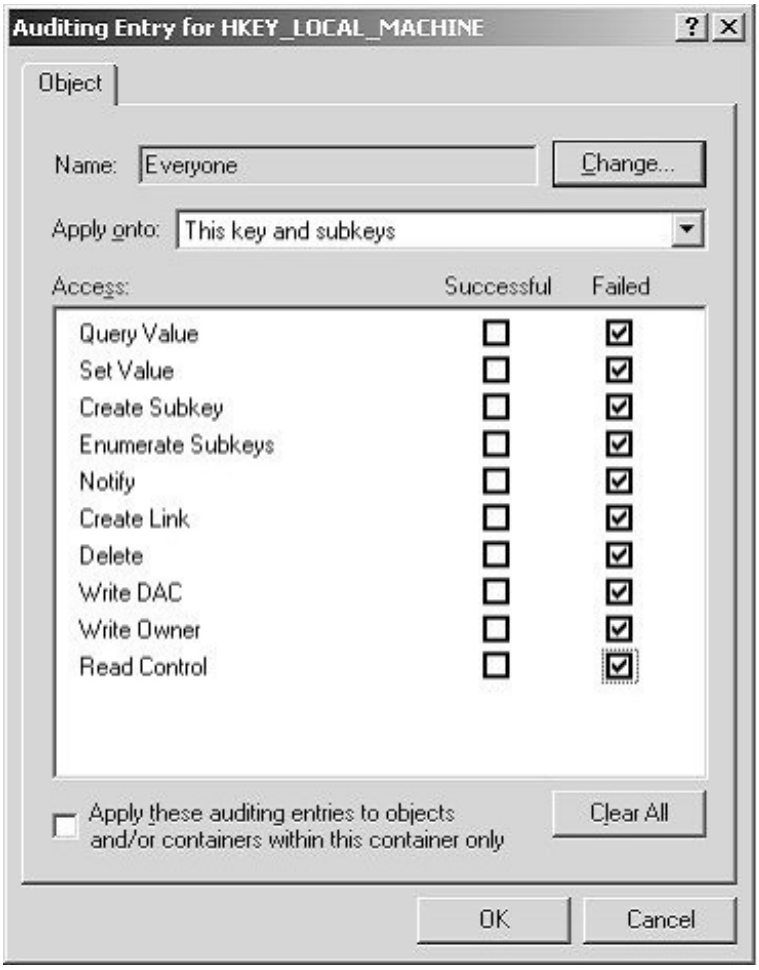
6.5 Registry Audit Settings

System auditing must be configured using the procedures outlined in the *NSA NT Guide,* Chapter 6, pages 33-34, and the *NSA WIN2K Guide: Security Configuration Tool Set,* Chapter 4, pages 27-28, for any registry auditing settings to be effective. Configure Registry auditing using the procedures found in the *NSA NT Guide,* Chapter 13, pages 82–83. (Equivalent procedures are not addressed in the NSA WIN2K guides). Registry auditing will be configured for the ***HKEY_LOCAL_MACHINE*** and ***HKEY_USERS*** hives. The following figure displays the required settings for DISA sites:



NOTE: ***Read Control*** *in the success column should not be checked on domain controllers, as this will generate excessive logging traffic.*

WIN2K:



NOTE: *Selecting* ***Read Control*** *in the success column on domain controllers will generate excessive logging traffic.*

This page is intentionally left blank.

7 GENERAL SECURITY MEASURES

7.1 DISA Physical Security Requirements

No computer will ever be completely secure if people other than the authorized users can physically access it. Ensure the following for maximum security on a mission critical computer that is not physically secure (locked safely away):

- *Workstations should have Complimentary Metal-Oxide Semiconductor (CMOS) level password protection enabled. Each TASO should implement procedures ensuring this level of security is applied to each PC/workstation under their charge. Corrupting the CMOS area will affect the entire computer, possibly making it unusable.*

- *The ISSO 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.)*

- *If the computer does not require network access, remove the network card. (SA)*

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 A* of the *Windows NT* and *Windows 2000 Checklists*. 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 WIN2K).

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.

- *Systems will be configured to automatically lock with a password-protected screen saver after inactivity of no more than 15 minutes. Five minutes is recommended. (SA)*

  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.*

- *Users will lock the system before leaving the server/workstation unattended.*

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 ISSO.
- 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 NT/WIN2K 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. 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 an NT machine so that they comply with security requirements.*

7.4 Installed Services

Windows NT/WIN2K 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 will configure services to run under local accounts with the minimum permissions and rights needed to perform their task.*

- *The SA will remove or disable unneeded or unknown services.*

- *If services are to be accessed remotely (e.g., FTP), the ISSO will ensure that a secure shell product is used to encrypt the userid and password, at a minimum. Encryption of the data is also highly recommended.*

7.4.1 Remote Shell Service (RSH)

A version of RSH, which ships with the Windows NT and WIN2K 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/WIN2K 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.

- *The SA will remove the service by typing **instsrv rshsvc remove** at the command prompt.*

7.4.2 Windows 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 NT/WIN2K 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 (e.g., Norton AntiVirus) may use the schedule service to run periodic scans on the local machine.

- *The ISSO will ensure that all schedule services are documented to include a list of users with access.*

- *If used, the schedule service will be configured to run under a local account. **(NT Only)*** 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.) (SA)*

NOTE 1: *Under Windows 2000 the Task Scheduler service must run under the System Account.*

NOTE 2: *If the account information on the Task Scheduler service is protected (grayed out), then the following procedure can be used to change it. This should only be done by a qualified, experienced SA who is comfortable working with the NT Registry:*

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.

7.4.3 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.

7.4.4 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 WIN2K. 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.

- *The sites will not deploy a Windows NT/WIN2K based Telnet server. (ISSO)*

- *Simple TCP/IP services will be disabled. (SA)*

7.4.5 Finger Service

Finger is a TCP/IP utility used to obtain information about a user account via a remote system. It can leave the system open to denial of service attacks. **Fingerd** is not native to Windows, but may be present. If this service is found, the **instsrv** tool, which ships with the Windows NT and WIN2K Resource Kits, can be used to remove the Finger service.

- *The SA will remove the service by typing **instsrv fingerd remove** at the command prompt.*

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 WIN2K 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.

- *The SA will remove the service by typing **instsrv rcmd remove** at the command prompt.*

7.4.7 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.

- *If SNMP is not required, the SA will disable the service.*

- *The SA will ensure that SNMP communities are used to secure data.*

7.4.8 Remote Registry Service (Windows 2000 Professional)

The Remote Registry Service allows you to change registry entries for a remote Windows 2000 computer (given the appropriate permissions). Disabling this service provides an extra level of protection to remote registries. (This is a Gold Standard setting.)

- *The SA will ensure that Remote Registry Service is disabled on Windows 2000 Professional machines.*

7.4.9 Automatic Updates Service (Windows 2000)

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

- *The SA will ensure that the Automatic Updates Service is disabled on Windows 2000 machines.*

7.4.10 Background Intelligent Transfer Service (BITs) (Windows 2000)

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. It is used by Windows Automatic Updates and other Microsoft products. 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 should be disabled to prevent users from downloading and installing updates that have not been approved by the site.

- *The SA will ensure that the Background Intelligent Transfer Service is disabled on Windows 2000 machines.*

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 DISA 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 DISA Field Security Operations *Desktop Application STIG* provides complete requirements for anti-virus software. Configure the product using that guidance.

- *An approved anti-virus product will be installed and enabled. (SA)*

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

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 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/WIN2K registry and Win32® security functions.

- *The default DCOM authorization level will be set at **connect** or above. (SA)*
- *Access permissions on DCOM objects will not permit non-administrators to create DCOM objects and execute code on the local system. (SA)*
- *Launch permissions on DCOM objects will not permit non-administrators to launch applications. (SA)*
- *Registry keys for DCOM objects will be configured with access permissions that prevent non-administrators from changing security settings. (SA)*

DCOMCNFG.EXE is in the **%systemroot%\System32** directory. It can be used to set access security on DCOM objects and specify the authorization level.

7.7 IP Forwarding

IP Forwarding is a feature of NT/WIN2K 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.

- *If IP forwarding is not allowed by the site's security policy, it will be disabled. (SA)*

7.8 Trusted Domains

Trusts are used by Windows NT/WIN2K 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.

7.9 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.

- *The Recycle Bin on servers **will** be configured to delete files immediately on delete. (SA)*

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.

7.10 Lightweight Directory Access Protocol (LDAP) - (WIN2K)

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 (WIN2K 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

- *An approved software configuration management tool will be used to manage the network in an automated and efficient manner. (ISSO)*
- *The ISSO will ensure that only an authorized SA has access to the configuration software.*
- *Access to software configuration installation disks or network installation share points will be restricted. (ISSO)*

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.

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

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

8.3 MQSeries

MQSeries is a communications utility developed by International Business Machines (IBM) that runs on multiple platforms (OS/390, UNIX, NT, WIN2K, 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.

DISA will initially use MQSeries to provide transaction processing between NT, WIN2K, UNIX, and IBM mainframe systems. MQSeries provides a mechanism for host and channel Identification and Authentication (I&A). Other security must be provided through user-supplied "**xit**" programs or channel security exits. There is no built-in mechanism to provide data encryption for messages (queries). Data encryption is accomplished with user-defined message exits. MQSeries will interface with native security systems to perform security I&A and access authority validation using the various security exits.

When MQSeries runs on NT/WIN2K, 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.

- *The MQSeries software will be installed in the default MQSeries directory. (SA)*

- *The MQSeries default local group account called MQM will be used. A Domain account with MQM in its name can be created if needed for MQSeries applications. The only user accounts allowed in either the local or domain MQM groups are those that need access to the MQSeries application. (SA)*

- *The access control permissions on the MQSeries directory, sub-directories, and files will be set in accordance with Appendix A of the NT and WIN2K SRR Checklists. (SA)*

- *MQSeries services will be configured to run under a **local account**, not the system account. (SA)*

- *The MQSeries log will be configured to preserve events and not overwrite. (SA)*

- *The Queue Manager log will be configured to preserve events and not overwrite. (SA)*

- *Versions of the older MQ.ini and QM.ini configuration files will be removed from the MQSeries\Config directory. (SA)*

- *The MCAUSER attribute on MQSeries Clients will contain a non-blank value or point to a security exit. (SA)*

8.4 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 and Windows 2000 operating systems for protecting sensitive information and for authenticating users.

The following are requirements for WebSphere Application Server to function properly in the Windows NT and WIN2K 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 NT 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 ISSO and SA will ensure that the following steps are taken:

- Create a separate security userid and grant the necessary permissions to perform administrative functions, for using the WebSphere Administrative Console (WAC) (SA)

- Configure WebSphere to use NT authentication in Windows NT domains. Configure it to use Active Directory for authentication in Windows 2000 domains. (SA)

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." The following files will have to be protected:

- Directories containing the JAVA programs, JAVA beans, JAVA servlets, and web applications used by WebSphere. Access will be limited to the WebSphere account and WebSphere administrators. (SA)

- 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, and must be protected. (SA)

- Directories containing the WebSphere Administrative Console functions. (SA)

- 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. (SA)

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

9 DISASTER RECOVERY

9.1 Uninterruptible Power Supply (UPS)

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

- *The ISSO or TASO will ensure that each Windows NT/WIN2K 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 WESTHEM Security Handbook, Section 3.11, Information Operations Condition (INFOCON).*

This page intentionally left blank

APPENDIX A. RELATED PUBLICATIONS

Government Publications

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

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 1.0, January 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 1.1, 22 January 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 WESTHEM Security Handbook, Version 3, 1 December 2000.

Network Infrastructure STIG, V4R1, 10 July 2002.

Web Services STIG, V3R1, 22 August 2002.

Desktop Application STIG, V1R1, 18 October 2002.

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

AXENT Technologies –	http://www.axent.com
DISA –	http://www.disa.mil
DISA Datahouse –	https://datahouse.disa.mil
DISA Field Security Operations –	https://guides.ritchie.disa.mil
DISA Information Assurance–	https://iase.disa.mil http://iase.disa.smil.mil (SIPRNet)
DOD-CERT –	http://www.cert.mil
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
Nortel (certifying authority) –	http://www.nortel.com/entprods/entrust/main.html
RSA Data Systems (encryption software) –	http://www.rsa.com
Vulnerability Compliance Tracking System (VCTS) –	https://vms.disa.mil
Vulnerability Compliance Tracking System (VCTS) (Secret and Confidential) –	https://vms.disa.smil.mil
Winserve –	http://www.winserve.com

This page is intentionally left blank

APPENDIX B. 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, 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/WIN2K machine to conform to the C2 recommendations of the *NSA NT* and *WIN2K Security Guides* and the Field Security Operations *NT/WIN2K Addendum*. The SCM/SCT utility is available from the web sites mentioned in *Section 1.8, 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

NOTE: *The configuration files on the configuration tool for WIN2K 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 WIN2K 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 NT with Administrator rights.

2. Insert the disk with the **FSOscm.exe** program. (**WIN2KSCM.exe** for WIN2K)

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 WIN2K Guides* recommendations:

On All Windows NT/WIN2K 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/WIN2K 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 Field Security Operations *NT 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 *WIN2K Guides* and the Field Security Operations *NT/WIN2K 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 WIN2K 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.***

WIN2K:

Use the procedure to load the modified Security Options file, as detailed earlier in this document in *Section 4, Securing the Registry and WIN2K Policies*.

APPENDIX C. WINDOWS NT - 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 November 2002. 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

DOD-CERT IAVM Bulletins (IAVB) -NT

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories (NT) - Antivirus

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories (NT) - Service Pack

Technical Advisory 1999-T-0011 - Fragmented Internet Group Management Protocol (IGMP)

DOD-CERT IAVM Technical Advisories (NT) - Hotfixes

Technical Advisory 1999-T-0017 - Microsoft TCP Initial Sequence Number Randomness Vulnerability

Technical Advisory 2000-T-0001 - Microsoft NT 4.0 Spoofed LPC Post Request Vulnerability

Technical Advisory 2000-T-0002 - Microsoft “Registry Permissions” Vulnerability

Technical Advisory 2000-T-0005 IP - Fragment Assembly Denial of Service Vulnerability

Technical Advisory 2002-T-0007 Unchecked buffer in MS Multiple UNC Provider Vulnerability

DOD-CERT IAVM Technical Advisories - Terminal Server

Technical Advisory 1999-T-0005 - Denial of Service Attack against Windows NT Terminal Server

IAVM BULLETINS FOR SERVICES AND APPLICATIONS

DOD-CERT IAVM Bulletins (IAVB) - DNS Server

IAVB 2000-B-0001 - Bind NXT Buffer Overflow

DOD-CERT IAVM Alerts (IAVM) - Exchange Server/E-mail

There are no applicable IAVM Alerts at this time.

DOD-CERT IAVM Bulletins (IAVB) - Exchange Server/E-mail

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories - Exchange Server/E-mail

Technical Advisory 1999-T-0004 - Microsoft Exchange Server (Encapsulated SMTP Address)

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

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories - Microsoft Applications

Technical Advisory 1999-T-0007 - Microsoft Jet/ODBC Technical Advisory

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

Technical Advisory 2000-T-0007 - Microsoft Office 2000 UA ActiveX Control

Technical Advisory 2000-T-0008 - Microsoft SQL Server 7.0 Password Vulnerability

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

Technical Advisory 2000-T-0012 - Office 2000 HTML Object Tag

Technical Advisory 2000-T-0014 - Excel Register.ID Function

Technical Advisory 2001-T-0013 – Malformed Excel or PowerPoint document can bypass Macro security

Technical Advisory 2002-T-0001 – Multiple Vulnerabilities with Microsoft SQL Server

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

DOD-CERT IAVM Bulletins (IAVB) – Web Servers

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

DOD-CERT IAVM Technical Advisories – Web Servers

Technical Advisory 1999-T-0003 - Microsoft Internet Information Server (IIS) Data Access Components

Technical Advisory 1999-T-0006 - Microsoft IIS Malformed HTTP Request Header

Technical Advisory 1999-T-0015 - Domain Resolution and FTP Download Vulnerabilities (IIS 4.0 only)

Technical Advisory 2000-T-0003 - Link View Server-Side Component Vulnerability (IIS)

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 2001-A-0015 – Multiple Vulnerabilities in IE 5.5 SP2 and IE 6.0

DOD-CERT IAVM Bulletins (IAVB) – Web Browsers

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

IAVM 2002-B-0001 - Multiple Vulnerabilities in IE 5.5 SP2 and IE 6.0

DOD-CERT IAVM Technical Advisories – Web Browsers

Technical Advisory 1999-T-0008 - Microsoft Virtual Machine Sandbox Vulnerability (IE)

Technical Advisory 1999-T-0013 - Microsoft Internet Explorer (ActiveX) Vulnerability

Technical Advisory 2000-T-0006 - Frame Domain Verification, Unauthorized Cookie Access and Malformed Component Attribute Vulnerabilities (IE)

Technical Advisory 2000-T-0010/0010.1 - Microsoft "IE Script" and "Office 2000 HTML Script"

Technical Advisory 2000-T-0011 - Malformed E-mail Header Vulnerability

Technical Advisory 2000-T-0013 - Scriplet Rendering Patches (IE)

Technical Advisory 2001-T-0001 – Outlook, Outlook Express Vcard Handler contains unchecked buffer

Technical Advisory 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.

DOD-CERT IAVM Bulletins (IAVB) - Other Applications

Technical Bulletin 2001-B-0002 – Vulnerability in HP OpenView and IBM NetView

Technical Bulletin 2001-B-0003 – ISS RealSecure %U Encoding Intrusion Detection System Bypass Vulnerability

DOD-CERT IAVM Technical Advisories - Other Applications

Technical Advisory 1999-T-0009 - Gauntlet Firewall 5.0 Denial of Service Vulnerability

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

Technical Advisory 2001-T-0009 – Norton AntiVirus LiveUpdate Host verification vulnerability

This page is intentionally left blank.

APPENDIX D. 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 November 2002. Refer to the current WIN2K checklist for the most up-to-date listing.

IAVM BULLETINS FOR WINDOWS 2000

DOD-CERT IAVM Alerts (WinOS) - AntiVirus

There are no applicable IAVM Alerts at this time.

DOD-CERT IAVM Bulletins (WinOS) -AntiVirus

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories (WinOS) - Antivirus

There are no applicable IAVM Technical Advisories at this time.

DOD-CERT IAVM Technical Alerts (WinOS) - Service Pack

There are no applicable IAVM Alerts at this time.

DOD-CERT IAVM Bulletins (WinOS) - Service Pack

Technical Bulletin 2000-B-0007 - HyperTerminal Buffer Overflow

DOD-CERT IAVM Technical Advisories (WinOS) - Service Pack

Technical Advisory 2000-T-0005 - IP Fragment Assembly Denial of Service Vulnerability

DOD-CERT IAVM Technical Alerts (WinOS) - Hotfixes

IAVM 2002-A-SNMP-003 – Multiple Simple Network Management Protocol Vulnerabilities

IAVM 2002-A-SNMP-005 – Multiple Simple Network Management Protocol Vulnerabilities

DOD-CERT IAVM Bulletins (WinOS) - Hotfixes

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories (WinOS) - Hotfixes

Technical Advisory 2002-T-0007 – Unchecked buffer in MS UNC Provider 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

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories - Microsoft Applications

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

Technical Advisory 2000-T-0007 - Microsoft Office 2000 UA ActiveX Control

Technical Advisory 2000-T-0008 - Microsoft SQL Server 7.0 Password Vulnerability

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

Technical Advisory 2000-T-0012 - Office 2000 HTML Object Tag

Technical Advisory 2000-T-0014 - Excel Register.ID Function

Technical Advisory 2001-T-0013 – Malformed Excel or PowerPoint document can bypass Macro security

Technical Advisory 2002-T-0001 – Multiple Vulnerabilities with Microsoft SQL Server

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

DOD-CERT IAVM Bulletins (IAVB) – Web Servers

There are no applicable IAVM Bulletins at this time.

DOD-CERT IAVM Technical Advisories – Web Servers

There are no applicable IAVM Technical Advisories at this time.

DOD-CERT IAVM Alerts (IAVM) – Web Browsers

IAVM 2001-A-0004 - Incorrect MIME Header Can Cause IE to Execute E-mail Attachment

IAVM 2001-A-0015 – Multiple Vulnerabilities in IE 5.5 SP2 and IE 6.0

DOD-CERT IAVM Bulletins (IAVB) – Web Browsers

Technical Bulletin 2000-B-0002 - Netscape Navigator Improperly Validates SSL Sessions

IAVM 2002-B-0001 - Multiple Vulnerabilities in IE 5.5 SP2 and IE 6.0

DOD-CERT IAVM Technical Advisories – Web Browsers

Technical Advisory 2000-T-0006 - Frame Domain Verification, Unauthorized Cookie Access, and Malformed Component Attribute Vulnerabilities (IE)

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

Technical Advisory 2000-T-0011 - Malformed E-mail Header Vulnerability

Technical Advisory 2000-T-0013 - Scriplet Rendering Patches (IE)

Technical Advisory 2001-T-0001 - Outlook, Outlook Express Vcard Handler Unchecked Buffer (IE)

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

DOD-CERT IAVM Alerts (IAVA) – DNS Server

There are no applicable IAVM Alerts at this time.

DOD-CERT IAVM Bulletins (IAVB) – DNS Server

Technical Bulletin 2000-B-0008 - BIND 8.2.2-P6 Denial of Service Vulnerabilities

DOD-CERT IAVM Technical Advisories – DNS Server

There are no applicable IAVM Technical Advisories at this time.

DOD-CERT IAVM Alerts (IAVM) - Other Applications

IAVM 2002-A-SNMP-006 – Multiple Simple Network Management Protocol Vulnerabilities in Servers and Applications.

DOD-CERT IAVM Bulletins (IAVB) - Other Applications

Technical Bulletin 2001-B-0002 – Vulnerability in HP OpenView and IBM Tivoli NetView

Technical Bulletin 2001-B-0003 – ISS RealSecure %U Encoding intrusion detection system bypass vulnerability.

DOD-CERT IAVM Technical Advisories - Other Applications

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

Technical Advisory 2001-T-0009 – Norton AntiVirus LiveUpdate Host verification vulnerability

APPENDIX E. 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 NT/WIN2K SRR Checklists, FSO NT/WIN2K Addendum, and NSA NT and WIN2K Security guides should be referred to in performing the installation.

Prior to installation, ensure the following:

☐ The location of all equipment is in a secured area in accordance with DISA 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 Hotfix(s).

- Current approved service pack
- Check for additional hotfixes issued.

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

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

☐ Obtain all IAVM bulletin information for NT 4.0 or WIN2K and applicable applications.

Installation:

Follow these steps to ensure STIG compliance when installing a Windows NT 4.0 / WIN2K Server or 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 NT 4.0 / WIN2K according to manufacturer instructions and site configuration requirements.

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

☐ Install current service pack and applicable hotfixes.

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

☐ Create 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, 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 Guides*, the *NT/WIN2K Addendum*, and/or the *NT and WIN2K Checklist, 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.
  - ❑ Maximum password age
  - ❑ Minimum password age
  - ❑ Minimum password length
  - ❑ Password uniqueness
  - ❑ Account lockout
  - ❑ Bad logon attempts

- Bad logon counter reset
- Lockout duration
- Logon before password change
- Forced disconnect when logon hours expire (DCs only)

☐ *****Configure FTP services.

- Enter Warning Banner into registry (whether FTP is used or not).

  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.

☐ Remove the OS2 and POSIX files.

☐ *****Copy the ENPASFLT.DLL to %root%\System32 directory.

☐ Configure the Registry.

☐ Set the file and directory permissions (access control list).

- System files
- Event logs

☐ Set the registry key permissions (access control list).

☐ Set the appropriate printer share permissions for locally installed printers.

☐ Configure installed services.

- Remove Remote Shell services.
- Disable Scheduler/Task Scheduler services.
- Disable Simple TCP/IP services.

- Disable Telnet services.
- Remove Fingerd services.
- Remove RCMD services.
- Disable SNMP services if not required.

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.

☐ Set Event log settings.

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

☐ Enable Auditing

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

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

☐ *****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.

- Refer to the *NSA Guides* and the *NT/WIN2K 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 F. GLOSSARY OF TERMS

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