MCAFEE VIRUSSCAN ENTERPRISE 8.8 SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 5, Release 7

24 July 2015

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA of any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

This McAfee Antivirus STIG provides the technical security policies, requirements, and implementation details for applying security concepts to Commercial-Off-The-Shelf (COTS) applications.

Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Malware has become the most significant external threat to most systems, causing widespread damage and disruption, and necessitating extensive recovery efforts within most organizations. Spyware malware's intention is to violate a user's privacy and has become a major concern to organizations. Although privacy violating malware has been in use for many years, it has become much more widespread recently, with spyware invading many systems to monitor personal activities and conduct financial fraud. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing, which is using deceptive computer-based means to trick individuals into disclosing sensitive information. Another common form is virus hoaxes, which are false warnings of new malware threats.

These requirements address several major forms of malware, including viruses, worms, Trojan horses, malicious mobile code, blended attacks, spyware tracking cookies, and attacker tools, such as backdoors and root kits.

1.1 Executive Summary

This document is a requirement for all DoD administered systems and all systems connected to DoD networks. These requirements are designed to assist Security Managers (SMs), Information Security System Managers (ISSMs), Information Security System Officers (ISSOs), and System Administrators (SAs) with configuring and maintaining security controls. This guidance supports DoD system design, development, implementation, certification, and accreditation efforts.

There are two individual STIG packages available for the McAfee VirusScan Enterprise 8.8:

- McAfee VirusScan Enterprise 8.8 Local Client
- McAfee VirusScan Enterprise 8.8 Managed Client

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provide an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will, **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any STIGs, SRGs, and other related security information. The address for the IASE site is http://iase.disa.mil/.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configurations settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system’s particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

2. GENERAL ANTIVIRUS GUIDANCE

2.1 AntiVirus Information

Next to properly configured operating system security controls, effective antivirus software is the most critical tool in securing desktop application systems. The value of updated software with current virus definition files cannot be underestimated. Malicious programs that result in a denial of service (DoS) or corruption of data can be thwarted with antivirus programs that look for signatures of known viruses and take preventative action.

The use of products by DoD organizations, other than those available on the DoD Patches Repository website, is discouraged. DoD has special licensing agreements with both McAfee and Symantec.

It must be noted that the guidelines in this section have been written to apply to clients whether on a server or workstation. Using these guidelines for mail servers does not provide appropriate or adequate protection for servers running complex applications (such as Microsoft Exchange or Lotus Notes). Additional antivirus measures need to be taken on mail servers.

The following sub-sections provide general guidance that applies to all antivirus software.

It is recommended that signatures files be updated daily.

2.2 General Guidance for Antivirus Software

This section details general guidance for the configurations of antivirus products.

Scans at boot time (or daily) are recommended when this would not cause a significant impact to operations.

The following file types are particularly vulnerable as the host for a virus. These file types must be included in the antivirus scan:

- Executable, service and driver files (i.e., files suffixed with .bat, .bin, .com, .dll, .exe, .sys, etc.)
- Application data files that could contain a form of mobile code (i.e., files suffixed with .doc, .dot, .rtf, .xls, .xlt, .hta, scrap objects, .wsh, etc.)

In the event that a virus is found, the user must be notified. This allows the user to take any additional action to reduce damage and halt propagation of the virus. The user should also exercise the appropriate computer security incident reporting requirements as defined by the site.

3. TECHNOLOGY OVERVIEW

This document, and associated STIG, has set forth requirements based upon having a secured Windows environment as described in various other documents. These documents include the NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations and NIST SP 800-83, Guide to Malware Incident Prevention and Handling available from National Institute of Standards and Technology (http://www.nist.gov) and the Windows STIG's available from the IASE website (http://iase.disa.mil/). Failure to follow these requirements can significantly diminish the value of many of the specifications in this document.

Security controls that are managed through the underlying operating system platform directly affect the strength of the security that surrounds desktop applications. This section highlights some measures that are taken to increase that strength.

This STIG will be updated quarterly, as needed. The audience of this STIG should be aware of the importance of keeping current with the Task Orders, Op Orders, and Fragmentation Orders issued by US CYBERCOM.

In the event a directive issued by US CYBERCOM results in a setting to be more restrictive than this STIG, the US CYBERCOM directive will take precedence over the STIG setting.

In the event a directive issued by US CYBERCOM results in a setting to be more relaxed than this STIG, this STIG's requirement will take precedence over the US CYBERCOM directive.

3.1 Changes in VSE 8.8

The VirusScan® Enterprise 8.8.0 release has been updated to include the following new features and enhancements:

- Enhanced performance.
- Allows ePolicy Orchestrator 4.5 or 4.6 to manage your VirusScan Enterprise systems.
- A new ScriptScan URL exclusion user interface has been added to allow configuring of these exclusions instead of manually editing ScriptScan settings in the registry.
- Support for Outlook 2010 email scanning.
- Support for Lotus Notes 8.0x through 8.5.1 email scanning.

3.2 McAfee VSE 8.8 Functionality

3.2.1 Access Protection

Access Protection (AP) is a behavior-blocking feature, also known as Zero Day Protection, with capability of blocking Ports, Files/Folders, and the Windows Registry. Each of these features has an associated kernel-level driver to filter the respective activity, and compares actions against a list of rules. Any action found to be in breach of a rule is acted upon. The action taken in response depends on what has been configured for the appropriate rule.

McAfee provides a number of helpful standard rules. Those we believe are essential are enabled by default. You can define your own rules as required.

3.2.2 Buffer Overflow Protection

Buffer Overflow Protection (BOP) monitors Application Program Interfaces, checking for code execution from a buffer overflow or buffer overrun. BOP does not stop the overrun from occurring, but will stop code execution that occurs from that overrun. This is a common exploit method, used by malware against vulnerable applications, to gain access to data or the system and/or to further propagate itself.

Protection is accomplished by having kernel-level hooks (also known as "kernel patching" of various system tables) detour code execution through our tests for safety, before returning to their previously scheduled programming.

Note: This feature is not supported on 64-bit platforms as its kernel cannot be "patched".

3.2.3 On-Access scan

A file system filter driver monitors all file activity and determines, based on configuration, whether a file object that is being accessed requires scanning. If so, the On-Access Scanner service (McShield.exe) processes the file object further to determine if exclusions are applicable. If they are not, the OAS service performs a scan and reports the results back to the filter driver. McShield.exe loads the McAfee Engine and DAT files into memory to facilitate scanning and actions taken on infected files.

3.2.1 On-Demand scan

On-Demand Scanning (ODS) in this release has been improved over prior versions by moving from single threaded scanning to multi-threaded scanning. This allows VSE 8.8 to complete scan tasks in a much shorter time. The file system is walked and file names are added to a scanning pool, from which an available scanning thread is retrieved and acted on. If a file is modified or written to disk after the scan had progressed past that part of the file system, it will not be scanned until next time the ODS is run. Multi-threaded scanning applies to the file system only. Available scanning threads may come from the McShield.exe process, you will therefore see McShield.exe as active when ODS runs instead of the expected Scan32 or Scan64 process. The configured settings for the ODS are still in effect for those threads however.

3.2.2 On-Access scan and On-Demand scan of archives

VSE scans each file in an archive. However, because there is no function for re-packing the archive, it is opened each time a file in the archive is scanned. Because archives cannot be re-packed, no actions can be taken on individual files within them. Therefore, if an infected file is detected within an archive, the entire archive is treated as an infected file.

4. MANUAL REVIEW

To conduct a manual review of compliance with the McAfee VirusScan Enterprise (VSE) 8.8 STIG requirements, it is necessary to use some tools that are provided with the Windows operating system. Some of these tools are as follows:

- Windows Explorer
- Windows "Edit File Type" facility – accessed through the Windows Explorer
- Windows Registry Editor – regedit.exe or regedt32.exe
- Windows Search – accessed via the Windows Start Menu
- Microsoft Management Console (MMC)
- Microsoft Security Configuration and Analysis snap-in (used with the MMC)

Additionally, many of the settings required in this document must be set using dialogs provided by the applicable application. Such dialogs would include the use of pull-down menus, tabs, and GUI windows.

Instructions for the manual remediation of vulnerabilities to include adding, deleting, and modifying settings can be found in the "Fix" information provided in the VMS vulnerability description.

4.1 McAfee MOVE vs. McAfee VirusScan Enterprise

McAfee Management for Optimized Virtual Environments (MOVE) is currently available and will DoD organizations may have deployed it to their virtual environment. A McAfee MOVE Multi-Platform 2.6 STIG has been released. A McAfee MOVE Agentless 3.0 STIG is will be released at a later date.

When McAfee MOVE is deployed by an organization for AntiVirus protection for the organization’s virtual infrastructure, McAfee VirusScan Enterprise will not be installed on those virtual machines which are scanned by a McAfee MOVE Offload Scan Server (OSS), in a McAfee MOVE MultiPlatform deployment, nor will McAfee VirusScan Enterprise be installed on those virtual machines which are scanned by a McAfee MOVE Security Virtual Appliance (SVA), in a McAfee MOVE Agentless deployment.

In such case where a system is being configured/reviewed which is part of a MOVE deployment, the McAfee MOVE STIG will be used for determing the AntiVirus posture of the virtual machine and the McAfee VirusScan Enterprise STIG will not be used.

In a McAfee MOVE MultiPlatform deployment, the OSS will be a Windows platform and will require McAfee VirusScan Enterprise 8.8 or higher to be installed and configured to the settings in this STIG. The virtual images, however, will only have the McAfee MOVE AV Client installed.

In a McAfee MOVE Agentless deployment, the SVA will be a hardened Linux appliance and will require McAfee VirusScan for Linux 1.7 or higher to be installed and configured to the settings found in the MOVE STIG package.

4.2 Conducting a Manual Review

The STIG documentation included in this package are written explicitly for McAfee VirusScan 8.8 Manual Review. In the event a major version or interim version revision is released from the vendor, either this STIG will be updated with pertinent changes, or a new STIG will be developed.

The Locally Configured STIG is to be used for those systems with McAfee VirusScan Enterprise 8.8 installed locally and for which the installation is not managed by the site’s McAfee HBSS ePO server.

The Managed Client STIG is to be used for those systems for which the McAfee VirusScan Enterprise 8.8 was deployed from the site’s McAfee HBSS ePO server.

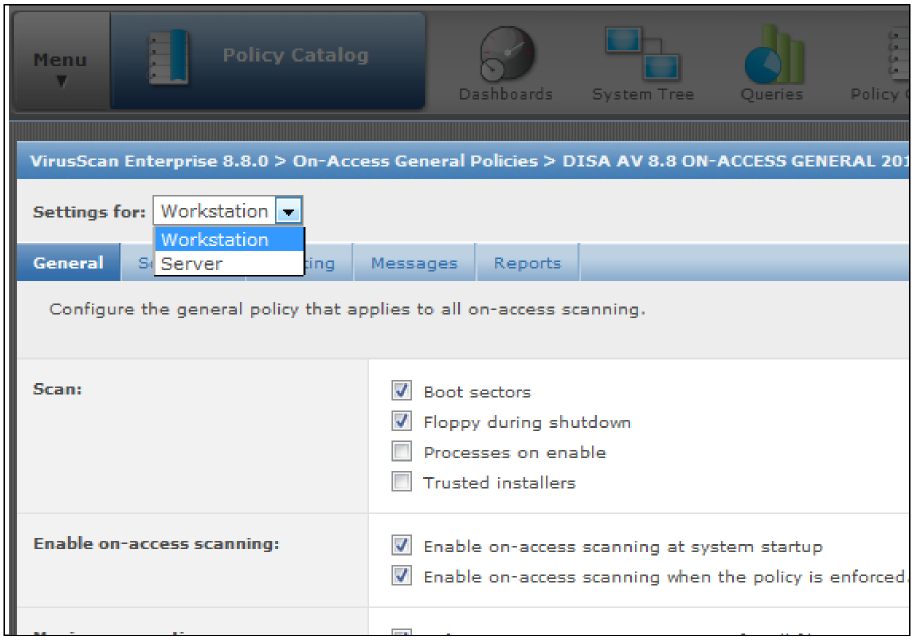
Note: While registry settings are provided in the STIG documentation, the intent is for the Manual reviews to be conducted within the respective interface, as specified in sections 4.2.2 and 4.2.3.

4.2.1 Server/Workstations Policies

When configuring McAfee VirusScan Enterprise policy settings within the McAfee ePolicy Orchestrator (ePO) server, the all VirusScan Enterprise policies will include both workstation and server settings.

Before configuring or reviewing a policy for a specific system, ensure the appropriate option is selection from the "Settings for:" drop-down list.

Figure 4-1: Choosing Workstation/Server Policy



VirusScan Enterprise 8.8.0 > On-Access General Policies > DISA AV 8.8 ON-ACCESS GENERAL 201

Settings for: Workstation

Workstation
Server

General | S | ing | Messages | Reports

Configure the general policy that applies to all on-access scanning.

Scan:
☑ Boot sectors
☑ Floppy during shutdown
☐ Processes on enable
☐ Trusted installers

Enable on-access scanning:
☑ Enable on-access scanning at system startup
☑ Enable on-access scanning when the policy is enforced

4.2.2 Locally Configured Manual Review

The Locally Configured Manual Review will be conducted locally on the system to which the McAfee VSE 8.8 has been installed. This review is not intended for those systems for which the McAfee VSE 8.8 was deployed from the McAfee HBSS ePO server.

To conduct the review, all checks will be reviewed by accessing the VSE 8.8 console of the system being reviewed.

The McAfee VSE 8.8 icon should be visible in the taskbar. If it is, right-click on the icon and choose to open the VirusScan Console.

If the McAfee VSE 8.8 icon is not in the taskbar, click on Start >> All Programs >> McAfee >> VirusScan Console.

Related registry keys are provided as a reference point and additional validation option. However, since the McAfee Host Intrusion Prevention and the VSE Access Protection modules might block some registry keys from being visible, the registry key method of review may produce false open findings.

4.2.3 Managed Client Manual Review

The Managed Client Manual Review will be conducted by accessing the McAfee HBSS ePO server from which the system being reviewed receives McAfee point product policies. In order to conduct a Managed Client Manual Review, an HBSS administrator will need to be available to assist during the review.

If access to the HBSS ePO server is not available, portions of the review can be conducted by following the Locally Configured Manual Review processes against the Managed client but because the VSE 8.8 is managed by the ePO server, many of the settings will be grayed out, making them inaccessible for review.

Related registry keys are provided as a reference point and additional validation option. However, since the McAfee Host Intrusion Prevention and the VSE Access Protection modules might block some registry keys from being visible, the registry key method of review may produce false open findings.

Specified file paths within the STIG may be hidden by default. If filepath is initially not found, verify it is not hidden before making requirement validation.

5. TERMINOLOGY CONVENTIONS

Current desktop applications present a graphical user interface (GUI) for their use and parameter customization. Most of the parameter settings specified in this document can be examined and changed through the application's GUI, subject to Windows policy settings. The following terms are used in describing how to view or configure the settings:

- Dialog - An application dialog is a window presented by the application.
- Menu - An application menu consists of a textual list of actions, commands, or (sometimes) options that can be selected.
- Enable - The term enable is used to describe the selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies "enable", the associated option button display would indicate that the option is selected.
- Disable - The term disable is used to describe the de-selection of a parameter setting, often indicated as an option button or check box in the application GUI. For example, when a parameter setting specifies "disable", the associated option button display would indicate that the option is de-selected.
- Select - Indicates highlight a specific topic or option. In some cases, selecting will toggle a setting. In other cases, selecting will merely highlight, allowing for other options to be configured for that selected object. It is important to determine which case applies by reading the directive in full.

6. NIST GUIDANCE FOR MALWARE HANDLING

The McAfee VSE 8.8 settings have been developed, in part, based upon guidance in *NIST 800-83, Guide to Malware Incident Prevention and Handling.*

Excerpt:

"Organizations should develop and implement an approach to malware incident prevention.

Organizations should plan and implement an approach to malware incident prevention based on the attack vectors that are most likely to be used, both currently and in the near future. Because the effectiveness of prevention techniques may vary depending on the environment (i.e., a technique that works well in a managed environment might be ineffective in a non-managed environment), organizations should choose preventive methods that are well suited to their environment and systems. An organization's approach to malware incident prevention should incorporate policy considerations, awareness programs for users and information technology (IT) staff, and vulnerability and threat mitigation efforts.

Organizations should ensure that their policies support the prevention of malware incidents.

An organization's policy statements should be used as the basis for additional malware prevention efforts, such as user and IT staff awareness, vulnerability mitigation, and security tool deployment and configuration. If an organization does not state malware prevention considerations clearly in its policy, it is unlikely to perform malware prevention activities consistently and effectively. Malware prevention-related policy should be as general as possible to allow flexibility in policy implementation and to reduce the need for frequent policy updates, but should also be specific enough to make the intent and scope of the policy clear. Malware prevention-related policy should include provisions related to remote workers. both those using systems controlled by the organization and those using systems outside of the organization's control (e.g., contractor computers, employees. home computers, business partners. computers, mobile devices).

Organizations should incorporate malware incident prevention and handling into their awareness programs.

Organizations should implement awareness programs that include guidance to users on malware incident prevention. All users should be made aware of the ways that malware spreads, the risks that malware poses, the inability of technical controls to prevent all incidents, and the importance of users in preventing incidents. Awareness programs should also make users aware of the policy and procedures that apply to malware incident handling, such as how to detect malware on a computer, how to report suspected infections, and what users might need to do to assist incident handlers. In addition, the organization should conduct awareness activities for IT staff involved in malware incident prevention and provide training on specific tasks.

Organizations should have vulnerability mitigation capabilities to help prevent malware incidents.

Organizations should have documented policy, processes, and procedures to mitigate operating system and application vulnerabilities that malware might exploit. Because vulnerability usually can be mitigated through one or more methods, organizations should use an appropriate combination of techniques, including patch management, application of security configuration guides and checklists, and additional host hardening measures so that effective techniques are readily available for various types of vulnerabilities.

Organizations should have threat mitigation capabilities to assist in containing malware incidents.

Organizations should perform threat mitigation efforts to detect and stop malware before it can affect its targets. The most commonly used threat mitigation technical control is antivirus software; NIST strongly recommends that organizations deploy antivirus software on all systems for which satisfactory antivirus software is available. To mitigate spyware threats, either antivirus software with the ability to recognize spyware threats or specialized spyware detection and removal utilities should be used on all systems for which satisfactory software is available. Additional technical controls that are helpful for malware threat mitigation include intrusion prevention systems, firewalls, routers, and certain application configuration settings. The System and Information Integrity family of security controls in NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, recommends having malware and spyware protection mechanisms on various types of hosts, including workstations, servers, mobile computing devices, firewalls, e-mail servers, and remote access servers.

Organizations should have a robust incident response process capability that addresses malware incident handling.

As defined in NIST Special Publication 800-61, Computer Security Incident Handling Guide, the incident response process has four main phases: preparation, detection and analysis, containment/ eradication/ recovery, and post-incident activity. Some major recommendations for malware incident handling, by phase or subphase, are as follows:

Preparation
Organizations should perform preparatory measures to ensure that they can respond effectively to malware incidents.

Detection and Analysis
Organizations should strive to detect and validate malware incidents rapidly because infections can spread through an organization within a matter of minutes.

Containment
Malware incident containment has two major components: stopping the spread of malware and preventing further damage to systems. Nearly every malware incident requires containment actions.

Eradication
The primary goal of eradication is to remove malware from infected systems.

Recovery
The two main aspects of recovery from malware incidents are restoring the functionality and data of infected systems and lifting temporary containment measures.

Post-Incident Activity
Because the handling of malware incidents can be extremely expensive, it is particularly important for organizations to conduct a robust assessment of lessons learned after major malware incidents to prevent similar incidents from occurring.

Organizations should establish malware incident prevention and handling capabilities that address current and short-term future threats.

Because new malware threats arise constantly, organizations should establish malware incident prevention and handling capabilities that are robust and flexible enough to address both current and short-term future threats and that can be modified and built on to address long-term future threats. Both malware and the defenses against malware continue to evolve, each in response to improvements in the other. For this reason, organizations should stay up-to-date on the latest types of threats and the security controls available to combat each type. As a new category of threats becomes more serious, organizations should plan and implement appropriate controls to mitigate it. Awareness of new and emerging threats and protective capabilities should be part of every organization's efforts to prevent malware incidents."

APPENDIX A: RELATED PUBLICATIONS

Government Publications

NIST SP 800-83, Guide to Malware Incident Prevention and Handling

NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations

Department of Defense, DoD Directive (DoDD) 8552.01, "Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems," 23 Oct 2006.

Department of Defense Instruction, "Department of Defense (DoD) Public Key Infrastructure (PKI) and Public Key (PK) Enabling", 24 May 2011.

Department of Defense, DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," October 24, 2002.

Department of Defense, DoD Instruction (DoDI) 8500.2, "Information Assurance (IA)," February 6, 2003.

Department of Defense, "X.509 Certificate Policy for the United States Department of Defense," Version 5.2, 13 November 2000.

Defense Information Systems Agency, "Secure Remote Computing Security Technical Implementation Guide", Current Version.

Executive Office of the President, Office of Management and Budget Memorandum, "Protection of Sensitive Agency Information", 23 June 2006.

National Security Agency (NSA), "E-mail Security in the Wake of Recent Malicious Code Incidents," Version 2.6, 29 January 2002.

National Security Agency (NSA), "Microsoft Office 2000 Executable Content Security Risks and Countermeasures," 8 February 2002.

National Security Agency (NSA), "Microsoft Office XP/2003 Executable Content Security Risks and Countermeasures," 10 February 2005.

Commercial Publications

McAfee VirusScan Enterprise 8.8 Software Installation Guide

McAfee VirusScan Enterprise 8.8 Best Practices Guide

Government Websites

http://www.disa.mil/	Defense Information Systems Agency
http://iase.disa.mil/ (NIPRNet)	Defense Information Systems Agency Information Assurance Support Environment
https://www.cybercom.mil (NIPRNet)	US CYBERCOM
http://www.nist.gov	National Institute of Standards and Technology
https://patches.csd.disa.mil	DoD Patch Repository
http://www.nsa.gov/isso/index.html	National Security Agency Information Assurance Directorate (NSA IAD)

Commercial and Other Non-government Sites

http://www.icsalabs.com/	International Computer Security Association (ICSA) Labs
http://mysupport.mcafee.com	McAfee Support
http://www.microsoft.com/download/en/default.aspx	Microsoft Download Center
http://windows.microsoft.com/en-US/internet-explorer/products/ie/home	Microsoft IE Product Downloads
http://technet.microsoft.com/en-us/security	Microsoft TechNet Security
http://www.wildlist.org/	The WildList Organization