# SCAP and
# Federal Desktop Core Configuration

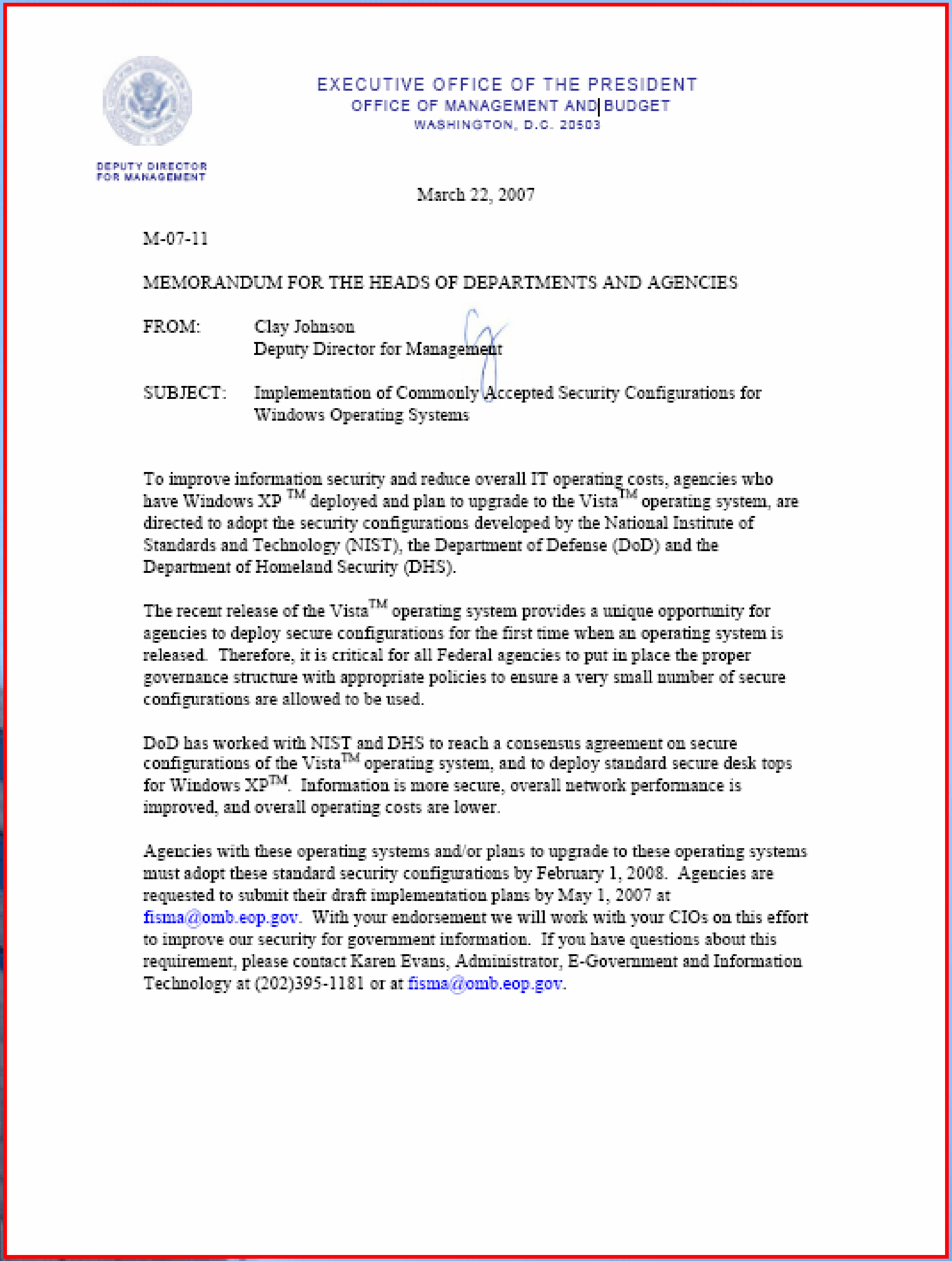
*presented by:*

Matt Barrett

National Institute of Standards and Technology

# OMB Memo M-07-11

*Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

March 22, 2007

M-07-11

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson
Deputy Director for Management

SUBJECT: Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

To improve information security and reduce overall IT operating costs, agencies who have Windows XP TM deployed and plan to upgrade to the Vista TM operating system, are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

The recent release of the Vista TM operating system provides a unique opportunity for agencies to deploy secure configurations for the first time when an operating system is released. Therefore, it is critical for all Federal agencies to put in place the proper governance structure with appropriate policies to ensure a very small number of secure configurations are allowed to be used.

DoD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista TM operating system, and to deploy standard secure desk tops for Windows XP TM. Information is more secure, overall network performance is improved, and overall operating costs are lower.

Agencies with these operating systems and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008. Agencies are requested to submit their draft implementation plans by May 1, 2007 at fisma@omb.eop.gov. With your endorsement we will work with your CIOs on this effort to improve our security for government information. If you have questions about this requirement, please contact Karen Evans, Administrator, E-Government and Information Technology at (202)395-1181 or at fisma@omb.eop.gov.

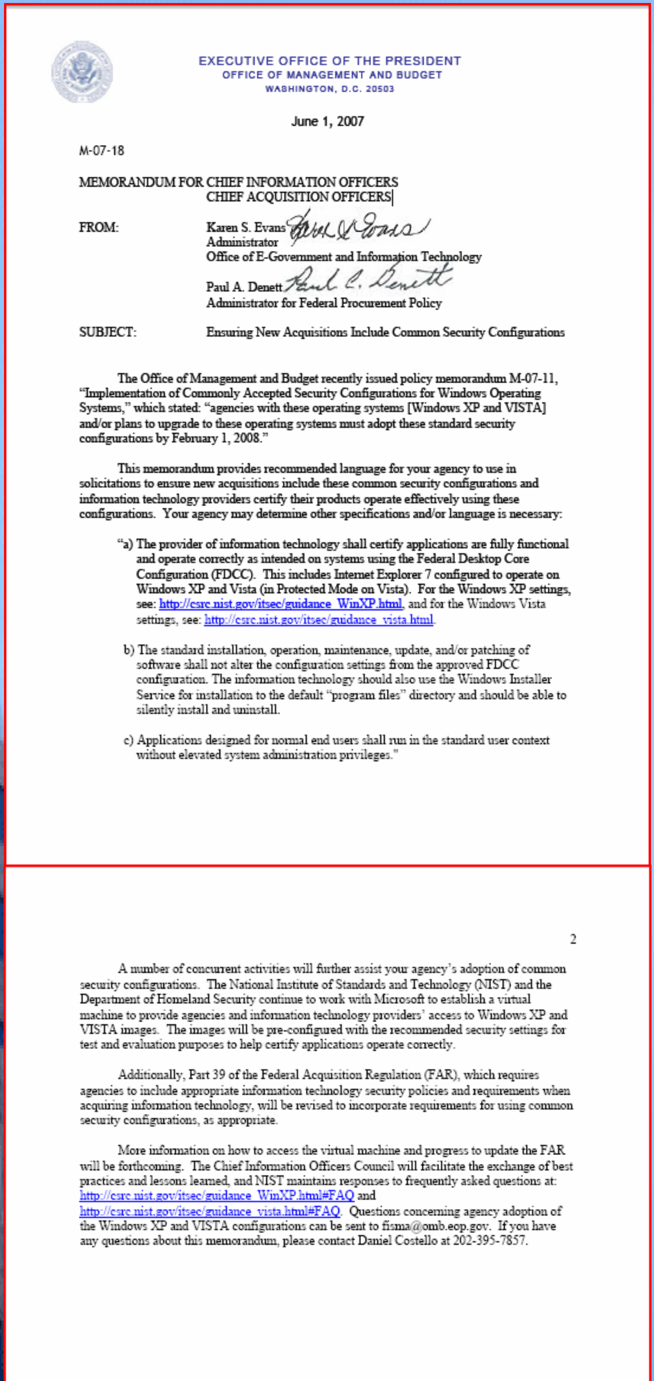
Corresponding OMB Memo to CIOs:

- Requires, “**Implementing and automating enforcement of these configurations;**”

•“NIST has established a program to develop and maintain common security configurations for many operating systems and applications, and **the “Security Content Automation [Protocol]” can help your agency use common security configurations.** Additionally, NIST’s revisions to Special Publication 800-70, “Security Configuration Checklist Program for IT Products,” will provide your agency additional guidance for implementing common security configurations. For additional information about NIST’s programs, please contact Stephen Quinn, at Stephen.Quinn@nist.gov.”

# OMB Memo M-07-18

***Ensuring New Acquisitions Include Common Security Configurations***



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 1, 2007

M-07-18

MEMORANDUM FOR CHIEF INFORMATION OFFICERS
CHIEF ACQUISITION OFFICERS

FROM: Karen S. Evans
Administrator
Office of E-Government and Information Technology

Paul A. Denett
Administrator for Federal Procurement Policy

SUBJECT: Ensuring New Acquisitions Include Common Security Configurations

The Office of Management and Budget recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008."

This memorandum provides recommended language for your agency to use in solicitations to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations. Your agency may determine other specifications and/or language is necessary:

"a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html, and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.

b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges."

2

A number of concurrent activities will further assist your agency's adoption of common security configurations. The National Institute of Standards and Technology (NIST) and the Department of Homeland Security continue to work with Microsoft to establish a virtual machine to provide agencies and information technology providers' access to Windows XP and VISTA images. The images will be pre-configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.

Additionally, Part 39 of the Federal Acquisition Regulation (FAR), which requires agencies to include appropriate information technology security policies and requirements when acquiring information technology, will be revised to incorporate requirements for using common security configurations, as appropriate.

More information on how to access the virtual machine and progress to update the FAR will be forthcoming. The Chief Information Officers Council will facilitate the exchange of best practices and lessons learned, and NIST maintains responses to frequently asked questions at: http://csrc.nist.gov/itsec/guidance_WinXP.html#FAQ and http://csrc.nist.gov/itsec/guidance_vista.html#FAQ. Questions concerning agency adoption of the Windows XP and VISTA configurations can be sent to fisma@omb.eop.gov. If you have any questions about this memorandum, please contact Daniel Costello at 202-395-7857.

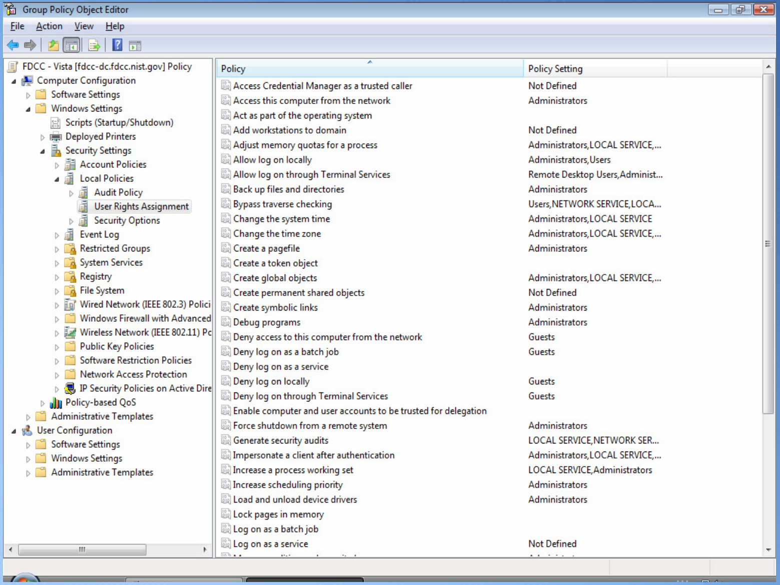
**"The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC).** This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista)."

"Applications designed for normal end users shall run in the standard user context **without elevated system administration privileges.**"

"The National Institute of Standards and Technology (NIST) and the Department of Homeland Security continue to work with Microsoft to **establish a virtual machine** to provide agencies and information technology providers' access to Windows XP and VISTA images. The images will be **pre-configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.** "

# Producing an FDCC Virtual Machine Image

Implement FDCC settings on virtual machine images



Group Policy Object Editor

- FDCC - Vista [fdcc-dc.fdcc.nist.gov] Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Polici
        - Windows Firewall with Advanced
        - Wireless Network (IEEE 802.11) Pc
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - IP Security Policies on Active Dire
      - Policy-based QoS
    - Administrative Templates
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

| Policy | Policy Setting |
|---|---|
| Access Credential Manager as a trusted caller | Not Defined |
| Access this computer from the network | Administrators |
| Act as part of the operating system | |
| Add workstations to domain | Not Defined |
| Adjust memory quotas for a process | Administrators,LOCAL SERVICE,... |
| Allow log on locally | Administrators,Users |
| Allow log on through Terminal Services | Remote Desktop Users,Administ... |
| Back up files and directories | Administrators |
| Bypass traverse checking | Users,NETWORK SERVICE,LOCA... |
| Change the system time | Administrators,LOCAL SERVICE |
| Change the time zone | Administrators,LOCAL SERVICE,... |
| Create a pagefile | Administrators |
| Create a token object | |
| Create global objects | Administrators,LOCAL SERVICE,... |
| Create permanent shared objects | Not Defined |
| Create symbolic links | Administrators |
| Debug programs | Administrators |
| Deny access to this computer from the network | Guests |
| Deny log on as a batch job | Guests |
| Deny log on as a service | |
| Deny log on locally | Guests |
| Deny log on through Terminal Services | Guests |
| Enable computer and user accounts to be trusted for delegation | |
| Force shutdown from a remote system | Administrators |
| Generate security audits | LOCAL SERVICE,NETWORK SER... |
| Impersonate a client after authentication | Administrators,LOCAL SERVICE,... |
| Increase a process working set | LOCAL SERVICE,Administrators |
| Increase scheduling priority | Administrators |
| Load and unload device drivers | Administrators |
| Lock pages in memory | |
| Log on as a batch job | |
| Log on as a service | Not Defined |

Use SCAP to verify FDCC settings were implemented correctly

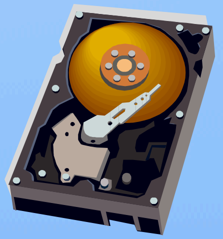
- Windows XP
- Windows Vista
- Windows XP Firewall
- Windows Vista Firewall
- Internet Explorer 7.0

ThreatGuard
Secutor prime free

secure elements®
audit. evaluate. comply.

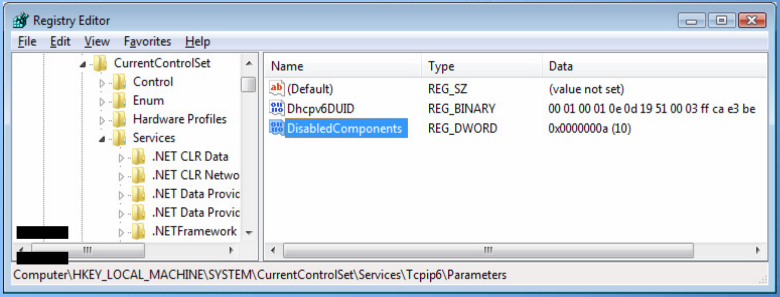
C5 Compliance Platform

Reconcile any “failed” SCAP tests



Record any exceptions

**FDCC Virtual Machine Image**



Registry Editor

- CurrentControlSet
  - Control
  - Enum
  - Hardware Profiles
  - Services
    - .NET CLR Data
    - .NET CLR Netwo
    - .NET Data Provic
    - .NET Data Provic
    - .NETFramework

[redacted]

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| Dhcpv6DUID | REG_BINARY | 00 01 00 01 0e 0d 19 51 00 03 ff ca e3 be |
| DisabledComponents | REG_DWORD | 0x0000000a (10) |

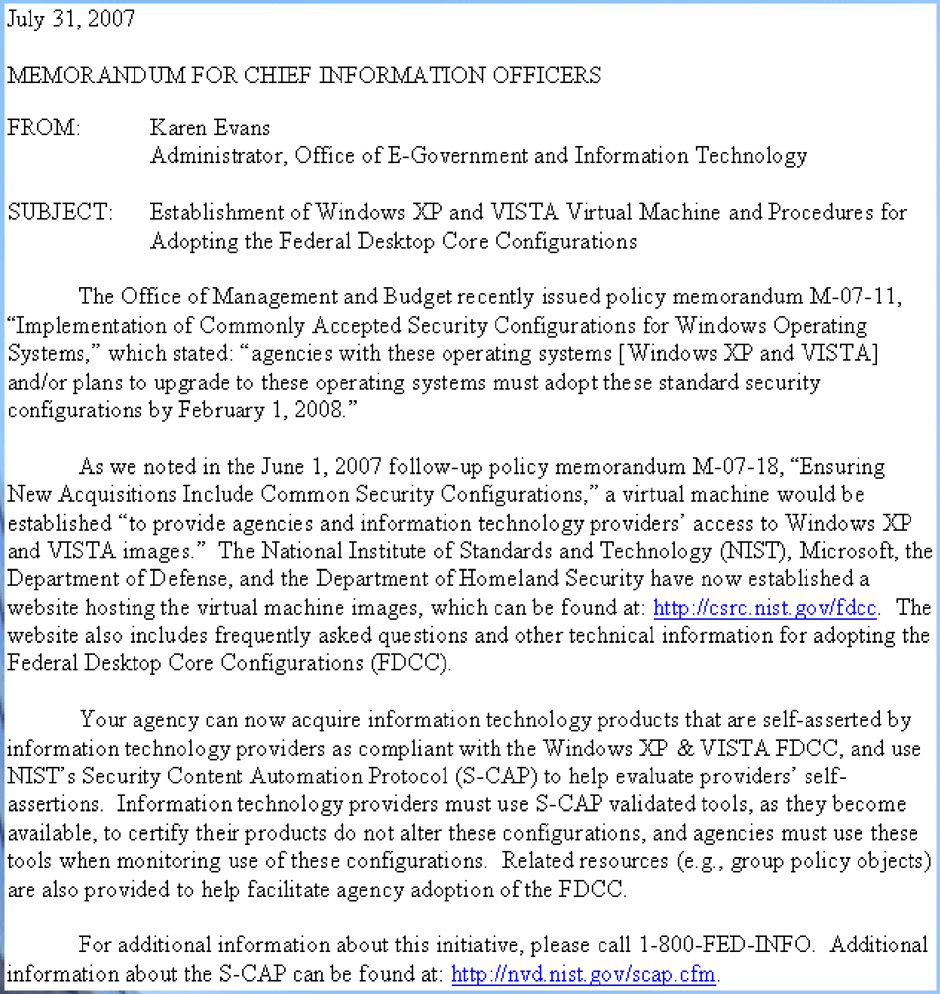
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters

NIST

# Test Lab Scenario

# OMB 31 July 2007 Memo to CIOs

## *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*



July 31, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations

The Office of Management and Budget recently issued policy memorandum M-07-11, “Implementation of Commonly Accepted Security Configurations for Windows Operating Systems,” which stated: “agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008.”

As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, “Ensuring New Acquisitions Include Common Security Configurations,” a virtual machine would be established “to provide agencies and information technology providers’ access to Windows XP and VISTA images.” The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc. The website also includes frequently asked questions and other technical information for adopting the Federal Desktop Core Configurations (FDCC).

Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST’s Security Content Automation Protocol (S-CAP) to help evaluate providers’ self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations. Related resources (e.g., group policy objects) are also provided to help facilitate agency adoption of the FDCC.

For additional information about this initiative, please call 1-800-FED-INFO. Additional information about the S-CAP can be found at: http://nvd.nist.gov/scap.cfm.

“As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, “Ensuring New Acquisitions Include Common Security Configurations,” **a virtual machine would be established “to provide agencies and information technology providers’ access to Windows XP and VISTA images.”** The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc.”

“Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and **use NIST’s Security Content Automation Protocol (S-CAP) to help evaluate providers’ self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations.”**

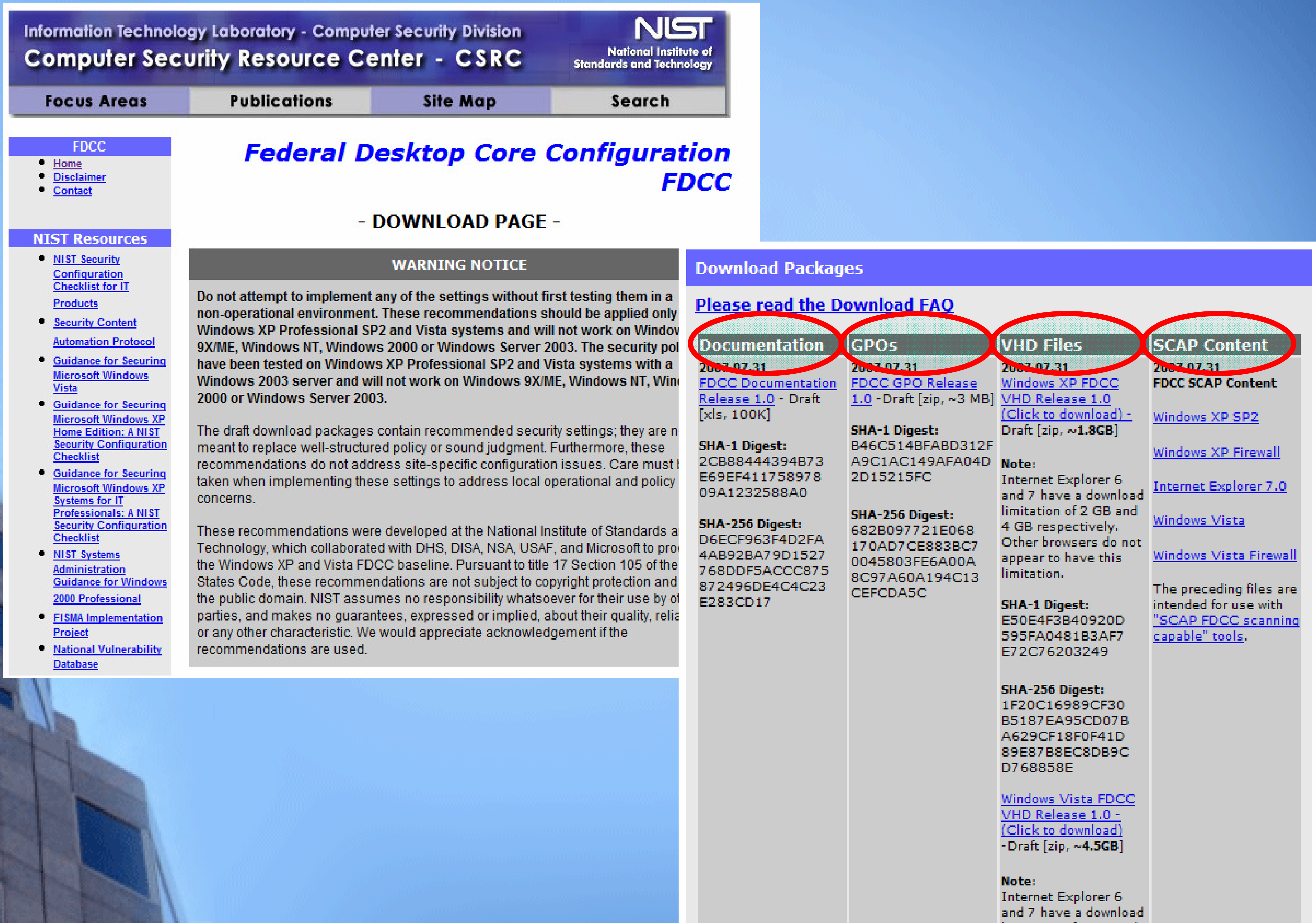
# Accomplishing FDCC with SCAP

| Operations Teams | Product Teams | Function |
|---|---|---|
| ● | ● | Test to ensure products do not change the FDCC settings |
| ● | | Assess new implementations for FDCC compliance |
| ● | | Monitor previous implementations for FDCC compliance |
| ● | | Generate FDCC compliance and deviation reports |

Quote from OMB Memo *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*
“**Information technology providers** must use S-CAP validated tools, as they become available, to **certify their products** do not alter these configurations, and **agencies** must use these tools **when monitoring** use of these configurations. “

# Test / Assess / Monitor Scenario

# http://csrc.nist.gov/fdcc/download_fdcc.html



Information Technology Laboratory - Computer Security Division

Computer Security Resource Center - CSRC

NIST National Institute of Standards and Technology

**FDCC**

- Home
- Disclaimer
- Contact

**NIST Resources**

- NIST Security Configuration Checklist for IT Products
- Security Content Automation Protocol
- Guidance for Securing Microsoft Windows Vista
- Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist
- Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist
- NIST Systems Administration Guidance for Windows 2000 Professional
- FISMA Implementation Project
- National Vulnerability Database

## Federal Desktop Core Configuration FDCC

### - DOWNLOAD PAGE -

**WARNING NOTICE**

**Do not attempt to implement any of the settings without first testing them in a non-operational environment. These recommendations should be applied only Windows XP Professional SP2 and Vista systems and will not work on Window 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The security pol have been tested on Windows XP Professional SP2 and Vista systems with a Windows 2003 server and will not work on Windows 9X/ME, Windows NT, Win 2000 or Windows Server 2003.**

The draft download packages contain recommended security settings; they are n meant to replace well-structured policy or sound judgment. Furthermore, these recommendations do not address site-specific configuration issues. Care must l taken when implementing these settings to address local operational and policy concerns.

These recommendations were developed at the National Institute of Standards a Technology, which collaborated with DHS, DISA, NSA, USAF, and Microsoft to pro the Windows XP and Vista FDCC baseline. Pursuant to title 17 Section 105 of the States Code, these recommendations are not subject to copyright protection and the public domain. NIST assumes no responsibility whatsoever for their use by ot parties, and makes no guarantees, expressed or implied, about their quality, relia or any other characteristic. We would appreciate acknowledgement if the recommendations are used.

**Download Packages**

**Please read the Download FAQ**

| Documentation | GPOs | VHD Files | SCAP Content |
|---|---|---|---|
| **2007.07.31**<br>FDCC Documentation Release 1.0 - Draft [xls, 100K]<br>**SHA-1 Digest:**<br>2CB88444394B73<br>E69EF411758978<br>09A1232588A0<br>**SHA-256 Digest:**<br>D6ECF963F4D2FA<br>4AB92BA79D1527<br>768DDF5ACCC875<br>872496DE4C4C23<br>E283CD17 | **2007.07.31**<br>FDCC GPO Release 1.0 -Draft [zip, ~3 MB]<br>**SHA-1 Digest:**<br>B46C514BFABD312F<br>A9C1AC149AFA04D<br>2D15215FC<br>**SHA-256 Digest:**<br>682B097721E068<br>170AD7CE883BC7<br>0045803FE6A00A<br>8C97A60A194C13<br>CEFCDA5C | **2007.07.31**<br>Windows XP FDCC VHD Release 1.0 (Click to download) - Draft [zip, ~**1.8GB**]<br>**Note:**<br>Internet Explorer 6 and 7 have a download limitation of 2 GB and 4 GB respectively. Other browsers do not appear to have this limitation.<br>**SHA-1 Digest:**<br>E50E4F3B40920D<br>595FA0481B3AF7<br>E72C76203249<br>**SHA-256 Digest:**<br>1F20C16989CF30<br>B5187EA95CD07B<br>A629CF18F0F41D<br>89E87B8EC8DB9C<br>D768858E<br>Windows Vista FDCC VHD Release 1.0 - (Click to download) -Draft [zip, ~**4.5GB**]<br>**Note:**<br>Internet Explorer 6 and 7 have a download | **2007.07.31**<br>**FDCC SCAP Content**<br>Windows XP SP2<br>Windows XP Firewall<br>Internet Explorer 7.0<br>Windows Vista<br>Windows Vista Firewall<br>The preceding files are intended for use with "SCAP FDCC scanning capable" tools. |

# FDCC Update Scenario