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

August 11, 2008

M-08-22

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

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

SUBJECT: Guidance on the Federal Desktop Core Configuration (FDCC)

In March 2007, OMB Memorandum M-07-11 announced the "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," directing agencies with Windows XP ™ deployed and/or plan to upgrade to the Vista ™ operating system to adopt the Federal Desktop Core Configuration (FDCC) security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

On June 20, 2008, NIST published the updated Federal Desktop Core Configuration Major Version 1.0 settings release. Relative to the previous version of FDCC which was originally posted in July 2007, 40 settings have changed. Changes were derived from public comment during the April and May 2008 public comment periods, analysis of the March 31, 2008, Agency FDCC reports and subject matter expertise. FDCC Major Version 1.0 settings are available at http://nvd.nist.gov/fdcc/download_fdcc.cfm.

Federal Desktop Core Configuration Major Version 1.0

FDCC Major Version 1.0 is based on Microsoft Windows XP Service Pack (SP) 2 and Microsoft Windows Vista SP 1. Although Security Content Automation Protocol (SCAP) Content has been engineered so that it will also operate on Windows XP SP3, near-term Windows XP patch checking will be oriented toward Windows XP SP2. It is understood that many managed environments throughout the Federal government implement service packs shortly after their release. While near-term Windows XP checking is based on Windows XP/SP2, we do not anticipate any significant measurement issues for Windows XP/SP3. NIST is currently working with IT product vendors to develop additional SCAP Content based on the FDCC settings for other platforms and applications.

To coincide with the release of FDCC Major Version 1.0, new SCAP Content has also been made available. This SCAP Content is inclusive of the 40 FDCC settings changes. At this time, the FDCC is comprised of settings located at http://fdcc.nist.gov that can be checked using the updated SCAP Content and SCAP-validated tools with FDCC Scanning capability as specified on the NIST website at http://nvd.nist.gov/scapproducts.cfm. Not all FDCC settings can be checked using automated scanning tools. NIST is coordinating the refinement of SCAP Content

to automate the checking of as many settings as possible and will release minor versions of SCAP Content as this work progresses.

New Microsoft-updated Group Policy Objects (GPO) and Virtual Hard Drive (VHD) files are also available. These files have been tested by NIST and made available at http://nvd.nist.gov/fdcc/download_fdcc.cfm.

The SCAP Validation Requirement

Both industry and government information technology providers must use SCAP validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings. Agencies will use SCAP tools to scan for both FDCC configurations and configuration deviations approved by department or agency accrediting authority. Agencies must also use these tools when monitoring use of these configurations as part of FISMA continuous monitoring[1].

The requirement for SCAP validated security software with a validation for FDCC scanning capability is a required component of the FDCC for several reasons including:

- SCAP validated tools enable centralized authorship, quality assurance and publication of a definitive security configuration in the form of a SCAP Checklist. SCAP Checklists enable repeatability of low level, technical test procedures for assessment and monitoring of FDCC settings, as long as a SCAP validated product processes them. Conversion of these test procedures into a wide variety of non-validated checklists and checklist processing technologies leaves significant room for translation error.
- SCAP validated tools also give IT providers the ability to present evidence that their product(s) do not alter FDCC settings in a common reporting format, SCAP XCCDF reports. Using this common standardized reporting format in conjunction with integrity checks of the SCAP Checklist and the IT product binaries used in the testing process will allow agencies to accept self-assertions with limited Federal testing. This could expedite procurement time.

For additional information on SCAP and a list of validated products go to http://nvd.nist.gov/scapproducts.cfm.

Compliance, Testing and Use of SCAP validated Tools for Application Providers Supporting the Federal Government

Federal CIOs shall ensure that government application providers self-assert currently supported versions of applications:

- Operate correctly on Federal Windows XP and Windows Vista computer systems configured with FDCC and
- Do not change FDCC settings.

[1] Continuous monitoring is discussed as a phase of the certification and accreditation process, specifically for testing controls, on pages 9 and 11 of the FISMA guidance, and is described in detail in NIST SP 800-37 and 800-53.

Consistent with NIST guidance, applications should be installed and configured according to the ordinary means utilized by the end client within the Federal computing environment. A typical IT provider testing scenario should include:

- Configure a system with the latest FDCC settings from the NIST website.
- Use a SCAP-validated tool with FDCC Scanner capability to baseline the initial configuration.
- Install the product and test common use cases (per normal processes).
- Use a SCAP-validated tool with FDCC Scanner capability to ensure the FDCC settings and patches are intact.
- Uninstall the application, reboot, and run a SCAP-validated tool with FDCC Scanner capability to ensure proper FDCC settings and patches are still present.

NIST recommends IT providers test applicable product versions with all relevant and current updates and patches installed, especially when the update is considered a "major version" change. It is assumed this would be accomplished by integrating FDCC-specific tests into pre-existing patch testing process. Self-assertions should be made for currently supported versions of a product. It is not necessary for vendors to issue additional self-assertion statements with every minor update or patch.

IT providers' self-assertion for the currently supported versions of an IT product is valid:

- As long as the asserted version of the application is supported or in use by a Federal agency;
- Regardless of patches or updates issued for Microsoft Windows XP, Windows Vista, Windows XP desktop firewall, Windows Vista desktop firewall or Internet Explorer 7.0;
- Regardless of how an agency deploys the self-asserted version of the application (on other systems, across networks, with other applications, etc.) agency integrators must ensure FDCC compliance throughout the integration process and
- Even if the tool used to test the IT product eventually loses its validation because the tool vendor elected not to re-validate that version of the software.

Changes to FDCC settings will affect self-assertions of IT products. IT providers will self-assert currently supported versions of IT products against the latest FDCC major version and future major versions. Future FDCC changes having minimal security impact may be released as minor versions to FDCC. Self-assertion is not required for minor releases.

Scope of "Desktop" Configuration

Microsoft Windows XP and Windows Vista are desktop operating systems. Accordingly, FDCC is applicable to all computing system using Windows XP and Windows Vista, including desktops and laptops but not including servers. It is important for the collective security of the Federal Government for all the Windows XP and Windows Vista computers to meet or exceed FDCC, regardless of function.

Regarding Microsoft Windows XP and Vista, IT Providers are not required to self-assert a) operating systems other than Microsoft Windows XP and Windows Vista or b) applications that

run on operating systems other than Microsoft Windows XP and Windows Vista. This includes server operating systems and applications.

Additionally, and in support of the deviation analysis process conducted in March 2008, OMB has provided five environments/system roles which agencies should map any given desktop using Windows XP and/or Vista. These five environments/system roles are: 1) Centrally Managed General Purpose Desktop, 2) Centrally Managed General Purpose Laptop, 3) Development System, 4) Special Use System, and 5) Other. More information on these categories can be found at http://nvd.nist.gov/fdcc/fdcc_reporting_faq_20080328.cfm. This report marks the first in a line of ongoing assessments to be conducted to determine compliance to FDCC through the use of SCAP validated tools.

It is important to note NIST is currently working with a number of IT vendors on standardizing security settings for a wide variety of IT products and environments. NIST Special Publication 800-68, "Guidance for Securing Microsoft Windows XP Systems for IT Professional: A NIST Security Configuration Checklist" also includes technology neutral configuration settings for a variety of email, web browser and firewall vendors.

NIST addresses various operating systems and applications through the NIST Security Configuration Checklists Program for IT Products. The NIST process for creating, vetting and making security checklists available for public use is documented in NIST SP 800-70, "Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers."

NIST will also continue to host workshops to foster a collaborative environment between Federal agencies and IT providers. The FDCC technical mailing list, fdcc@nist.gov, and SCAP mailing lists such as scapdev@ nist.gov and scap-content@nist are also forums to discuss FDCC issues.

Revised Part 39 of the Federal Acquisition Regulation (FAR)

On February 28, 2008, revised Part 39 of the Federal Acquisition Regulation (FAR) was published which reads:

> PART 39-ACQUISITION OF INFORMATION TECHNOLOGY
> 1. The authority citation for 48 CFR part 39 continues to read as follows: Authority: 40 U.S.C. 121(c); 10U.S.C. chapter 137; and 42 U.S.C. 2473(c).
> 2. Amend section 39.101 by revising paragraph (d) to read as follows:
> 39.101 Policy.
>
> * * * * *
> (d) In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated.
>
> [BILLING CODE 6820-EP]

Technology Infrastructure Subcommittee – FDCC Change Control Board

With the release of the FDCC comes the creation of the Technology Infrastructure Subcommittee (TIS). This subcommittee will convene under the Federal Chief Information Officer (CIO) Council's Architecture and Infrastructure Committee (AIC). This subcommittee will convene under the Federal CIO Council's Architecture and Infrastructure Committee (AIC). The TIS will be responsible for coordinating the Federal CIO Council FDCC Change Control Board. The TIS is currently finalizing its charter which will be available at the end of August.

Although we anticipate relatively few and infrequent changes to FDCC settings, the Change Control Board will provide a unified process and perspective from the Federal CIO community on proposed updates, standards and guidance to consider and adjudicate potential changes to the FDCC in the future. The TIS will work in conjunction with NIST to assist with comprehensive analysis and public review process. In order to ensure appropriate roles and responsibilities, the TIS is currently developing a FDCC Concept of Operations that will describe relationships with NIST and other standards bodies as well as the change control process. This document will be finalized by early fall.

FISMA Guidance

Per OMB Memorandum M-08-21, "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," the following configuration management questions are provided regarding FDCC:

c. Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:
    - c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.
    - c.2. New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology," is included in all contracts related to common security settings. Yes or No.
    - c.3. All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.

http://www.whitehouse.gov/omb/memoranda/fy2008/m08-21.pdf

Policy Utilization Effort

OMB in conjunction with the General Services Administration (GSA) has initiated the Policy Utilization Assessment (PUA) effort. The PUA is intended to provide a service offering to assist CIOs in conducting independent assessments of IT security policy implementations, with FDCC being one of the first policy areas.

The program entails the use of statistical sampling (polling of agencies) to determine consistency of compliance to policy. Sampling activities will seek to collect policy implementation diagnostics and identify best practices and potential improvements to processes used by agency

CIOs to internally assess policy implementation progress. Through this effort, we will be able to identify gaps in current agency implementations, determine policy utilization percentages government-wide and increase agency confidence levels that results are being reached. The pilot assessments were completed in summer 2008.

Based on the pilot assessments, best practices and assessment methodologies will be shared with agencies to provide actionable insights and best practices to the CIOs.

If you should have any questions regarding the Federal Desktop Core Configuration, please email egov@omb.eop.gov.

Policy References:

M-07-11 -- "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems"
www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf

M-07-18 -- "Ensuring New Acquisitions Include Common Security Configurations"
www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf