

March 2010

INFORMATION SECURITY

Agencies Need to Implement Federal Desktop Core Configuration Requirements



GAO

Accountability * Integrity * Reliability



Highlights of [GAO-10-202](#), a report to congressional requesters

Why GAO Did This Study

The increase in security incidents and continuing weakness in security controls on information technology systems at federal agencies highlight the continuing need for improved information security. To standardize and strengthen agencies' security, the Office of Management and Budget (OMB), in collaboration with the National Institute of Standards and Technology (NIST), launched the Federal Desktop Core Configuration (FDCC) initiative in 2007.

GAO was asked to (1) identify the goals, objectives, and requirements of the initiative; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiative; and (3) identify the benefits, challenges, and lessons learned in implementing this initiative. To accomplish this, GAO reviewed policies, plans, and other documents at the 24 major executive branch agencies; reviewed OMB and NIST guidance and documentation; and interviewed officials.

What GAO Recommends

GAO recommends that OMB, among other things, issue guidance on assessing the risks of deviations and monitoring compliance with FDCC. GAO also recommends that 22 agencies take steps to fully implement FDCC requirements. These agencies generally concurred with GAO's recommendations.

To view the full product, including the scope and methodology, click on [GAO-10-202](#). For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

INFORMATION SECURITY

Agencies Need to Implement Federal Desktop Core Configuration Requirements

What GAO Found

The goals of FDCC are to improve information security and reduce overall information technology operating costs across the federal government by, among other things, providing a baseline level of security through the implementation of a set of standard configuration settings on government-owned desktop and laptop computers (i.e., workstations). To carry out the initiative, OMB required that executive branch agencies take several actions, including: (1) submit an implementation plan to OMB; (2) apply all configuration settings to all applicable workstations by February 2008; (3) document any deviations from the prescribed settings and have them approved by an accrediting authority; (4) acquire a specified NIST-validated tool for monitoring implementation of the settings; (5) ensure that future information technology acquisitions comply with the configuration settings; and (6) submit a status report to NIST.

While agencies have taken actions to implement these requirements, none of the agencies has fully implemented all configuration settings on their applicable workstations. Specifically, most plans submitted to OMB did not address all key implementation activities; none of the agencies implemented all of the prescribed configuration settings on all applicable workstations, though several implemented agency-defined subsets of the settings; several agencies did not fully document their deviations from the settings or establish a process for approving them; six agencies did not acquire and make use of the required tool for monitoring FDCC compliance; many agencies did not incorporate language into contracts to ensure that future information technology acquisitions comply with FDCC; and many agencies did not describe plans for eliminating or mitigating their deviations in their compliance reports to NIST. Until agencies ensure that they are meeting these FDCC requirements, the effectiveness of the initiative will be limited.

FDCC has the potential to increase agencies' information security by requiring stricter security settings on workstations than those that may have been previously in place and standardizing agencies' management of workstations, making it easier to manage changes such as applying updates or patches. In addition, a number of lessons can be learned from the management and implementation of the FDCC initiative which, if considered, could improve the implementation of future versions of FDCC or other configuration efforts. At the same time, agencies face several ongoing challenges in fully complying with FDCC requirements, including retrofitting applications and systems in their existing environments to comply with the settings, assessing the risks associated with deviations, and monitoring workstations to ensure that the settings are applied and functioning properly. As OMB moves forward with the initiative, understanding the lessons learned as well as the ongoing challenges agencies face will be essential in order to ensure the initiative is successful in ensuring public confidence in the confidentiality, integrity, and availability of government information.

Contents

Letter		1
	Background	3
	FDCC Aims to Improve Agencies' Information Security and Reduce IT Operating Costs	8
	Agencies Have Not Fully Implemented FDCC Settings, but Most Have Complied with Other Requirements	13
	Implementing FDCC Resulted in Benefits and Lessons Learned, but Agencies Continue to Face Challenges in Meeting Requirements	23
	Conclusions	34
	Recommendations for Executive Action	35
	Agency Comments and Our Evaluation	36
Appendix I	Objectives, Scope, and Methodology	41
Appendix II	Percentage of Agency Workstations with FDCC Settings Implemented as of September 2009	43
Appendix III	Recommendations to Departments and Agencies	45
Appendix IV	Comments from the U.S. Department of Agriculture	52
Appendix V	Comments from the Department of Commerce	53
Appendix VI	Comments from the Department of Defense	55
Appendix VII	Comments from the General Services Administration	57

Appendix VIII	Comments from the Department of Homeland Security	58
Appendix IX	Comments from the Department of Housing and Urban Development	61
Appendix X	Comments from the Department of the Interior	64
Appendix XI	Comments from the Department of Labor	65
Appendix XII	Comments from the National Aeronautics and Space Administration	68
Appendix XIII	Comments from the Office of Personnel Management	70
Appendix XIV	Comments from the Social Security Administration	73
Appendix XV	Comments from the Department of the Treasury	76
Appendix XVI	Comments from the U.S. Agency for International Development	77
Appendix XVII	Comments from the Department of Veterans Affairs	79

Tables

Table 1: Number of Agency FDCC Implementation Plans That Addressed Required Actions	14
Table 2: Range of the Number of Less-Stringent Deviations with the Corresponding Number of Agencies	17
Table 3: Ten Most Common Less-Stringent FDCC Deviations at Federal Agencies	17
Table 4: Status of Agency Compliance with Deviation Guidance	19
Table 5: Status of Agency Acquisition and Use of a NIST-validated SCAP Tool	20
Table 6: Agency Incorporation of Language into Contracts	22
Table 7: Agency-Reported Percentages of Workstations with FDCC Settings Implemented as of September 2009	43

Figure

Figure 1: Agency-Reported Implementation of FDCC Baseline as of September 2009	16
--	----

Abbreviations

FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act of 2002
IT	information technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SCAP	Security Content Automation Protocol

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office
Washington, DC 20548

March 12, 2010

The Honorable Joseph I. Lieberman
Chairman
The Honorable Susan M. Collins
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate

The Honorable Thomas R. Carper
Chairman
Subcommittee on Federal Financial
Management, Government Information,
Federal Services, and International Security
Committee on Homeland Security
and Governmental Affairs
United States Senate

The frequency of information security incidents at federal agencies, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology all contribute to the urgency of protecting the federal government's information and systems. In addition to these threats, we have consistently identified significant weaknesses in the security controls on federal systems, including desktops and laptops (i.e., workstations) that have impacted the confidentiality, integrity, and availability of government information. Due to the persistent nature of these vulnerabilities and associated risks, we have designated information security as a governmentwide high-risk issue since 1997 in our biennial reports to Congress.¹

In an attempt to standardize and thereby strengthen information security, the Office of Management and Budget (OMB) launched the Federal Desktop Core Configuration (FDCC) initiative in March 2007. The initiative mandated that federal agencies implement standardized configuration settings on workstations with Windows XP or Vista operating systems.

¹Most recently, GAO, *High-risk Series: An Update*, [GAO-09-271](#) (Washington, D.C.: January 2009).

In view of the importance of FDCC in improving the ability of the federal government to safeguard its systems and protect sensitive information, you asked us to (1) identify the goals, objectives, and requirements for the initiative; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiative; and (3) identify the benefits, challenges, and lessons learned in implementing this initiative.

We conducted our review at each of the 24 major federal agencies² covered by the Chief Financial Officers Act,³ where we obtained and analyzed policies, plans, status reports, and agency descriptions of challenges relative to the requirements of the initiative. We also developed a data collection instrument to gather information on the status of FDCC implementation at the 24 agencies as of September 2009. We compared agency documentation and descriptions of challenges with OMB program requirements and relevant National Institute of Standards and Technology (NIST) guidance, which we confirmed through interviews with OMB and NIST officials. We also met with staff from all 24 Offices of the Inspector General regarding their audit work performed relative to the initiative to obtain information on their audit methodology, findings, and related documentation. Based on our review of the adequacy of work performed, we have sufficient assurance to rely on work completed by the inspectors general in the context of our audit objective related to whether the agency had documented deviations and had incorporated language related to use of FDCC settings into its contracts.

We conducted this performance audit from December 2008 to March 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Further details of our objectives, scope, and methodology are included in appendix I.

²The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

³31 U.S.C. § 901.

Background

Cyber-based threats to federal systems and critical infrastructure are evolving and growing. These threats can be intentional or unintentional, targeted or non-targeted, and can come from a variety of sources, including criminals, terrorists, and other adversarial groups, as well as hackers and disgruntled employees. These potential attackers have a variety of techniques at their disposal, which can vastly enhance the reach and impact of their actions. For example, cyber attackers do not need to be physically close to their targets, their attacks can cross state and national borders, and they can preserve their anonymity. Further, the growing interconnectivity among different types of information systems presents increasing opportunities for such attacks. Reports of security incidents from federal agencies are on the rise, increasing by more than 200 percent from fiscal year 2006 to fiscal year 2008.⁴

In February 2009, the Director of National Intelligence testified that foreign nations and criminals had targeted government and private sector networks to potentially disrupt or destroy them, and that terrorist groups had expressed a desire to use cyber attacks as a means to target the United States.⁵ As recently as July 2009, media accounts reported that a widespread and coordinated attack over the course of several days targeted Web sites operated by major government agencies, including the Departments of Homeland Security and Defense, the Federal Aviation Administration, and the Federal Trade Commission, causing disruptions to the public availability of government information. Such attacks highlight the importance of developing a concerted response to safeguard federal information systems.

Previously Reported Weaknesses in Agency Information Security Controls

Compounding the growing number and kinds of threats, we—along with agencies and their inspectors general—have identified significant weaknesses in the security controls on federal information systems,⁶ which have resulted in pervasive vulnerabilities. These include

⁴GAO, *Information Security: Agencies Make Progress in Implementation of Requirements, but Significant Weaknesses Persist*, [GAO-09-701T](#) (Washington, D.C.: May 19, 2009).

⁵Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Washington, D.C.: Feb. 12, 2009).

⁶GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, [GAO-09-546](#) (Washington, D.C.: July 17, 2009).

deficiencies in the security of financial systems and information and vulnerabilities in other critical federal information systems and networks. These weaknesses exist in all major categories of information security controls at federal agencies; for example, in fiscal year 2008, weaknesses were reported in such controls at 23 of the 24 major agencies. Specifically, agencies did not consistently authenticate users to prevent unauthorized access to systems; apply encryption to protect sensitive data; and log, audit, and monitor security-relevant events, among other actions.

Our recent work focusing on specific agencies has also revealed security weaknesses, as illustrated by the following examples:

- In 2009, we reported that three National Aeronautics and Space Administration centers had not, among other things, sufficiently restricted system access and privileges to only those users that needed access to perform their assigned duties, appropriately implemented encryption to safeguard sensitive information, and expeditiously applied a critical operating system patch or patches for a number of general third-party applications.⁷ At the same time, the agency experienced numerous cyber attacks and malicious software infections, thereby exposing critical and sensitive data to unauthorized access, disclosure, and manipulation. We recommended that the agency take steps to mitigate these weaknesses and fully implement a comprehensive information security program.
- In the same year, we reported that the Financial Crimes Enforcement Network, a bureau within the Department of the Treasury, had not consistently implemented effective password controls or effectively controlled user identification and authentication.⁸ As a result, there was increased risk that malicious individuals could gain inappropriate access to sensitive systems and data. We recommended that the agency take steps to fully implement an agencywide security program.
- In 2008, we reported that although the Department of Energy's Los Alamos National Laboratory—one of the nation's weapons laboratories—had implemented measures to enhance the information security of its unclassified network, there were still vulnerabilities in monitoring and

⁷GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key Networks*, [GAO-10-4](#) (Washington, D.C.: Oct. 15, 2009).

⁸GAO, *Information Security: Further Actions Needed to Address Risks to Bank Secrecy Act Data*, [GAO-09-195](#) (Washington, D.C.: Jan. 30, 2009).

auditing compliance with security policies and controlling and documenting changes to a computer system's hardware and software.⁹

- Finally, we reported in 2007 that the Department of Homeland Security had significant weaknesses in computer security controls intended to protect the information systems used to support its U.S. Visitor and Immigration Status Indicator Technology program for border security.¹⁰ For example, the department had not implemented controls to effectively prevent, limit, and detect access to computer networks, systems, and information. Specifically, it had not provided adequate logging or user accountability for the mainframe, workstations, or servers and had not consistently maintained secure configurations on the application servers and workstations at a key data center and points of entry.

In each of these cases, we made recommendations for strengthening or fully implementing agencies' information security programs.

Federal Law Assigns Responsibility to OMB, NIST, and Agencies for Information Security

In addition to the responsibilities of individual agencies, OMB and NIST play key roles in ensuring the security of federal systems and information. Under the Federal Information Security Management Act of 2002 (FISMA),¹¹ OMB is responsible for developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, and reviewing agency information security programs at least annually. In addition, the act requires that OMB report to Congress no later than March 1 of each year on the status of agency compliance with FISMA. The act, which sets forth a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets, also assigned NIST responsibility for developing standards and guidelines (for systems other than national security systems) that include minimum information security requirements. FISMA also assigns specific responsibilities to agencies to document and implement agencywide security programs and report on

⁹GAO, *Information Security: Actions Needed to Better Protect Los Alamos National Laboratory's Unclassified Computer Network*, [GAO-08-1001](#) (Washington, D.C.: Sept. 9, 2008).

¹⁰GAO, *Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program*, [GAO-07-870](#) (Washington, D.C.: Jul. 13, 2007).

¹¹Enacted as title III of the E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

their security policies, procedures, and practices. For example, agencies are responsible for developing and complying with minimally acceptable system configuration requirements. Finally, FISMA requires agency inspectors general to annually evaluate agency information security activities.

OMB Initiated FDCC and Provided Guidance for Agency Implementation

To help carry out its responsibilities for ensuring federal information security, OMB launched the FDCC initiative in March 2007. This initiative required federal agencies to implement common security configurations on Windows XP and Vista operating systems¹² by February 2008.¹³ Subsequently, OMB issued several other memorandums detailing additional requirements and guidance to agencies on completing implementation of the initiative. OMB also has responsibility for approving any changes to the settings or setting parameters.

At the request of OMB, NIST published the first beta version of the FDCC configuration settings in July 2007 for federal workstations that use Windows XP or Windows Vista as their operating system. FDCC was based on settings developed by the Air Force in partnership with the National Security Agency, Defense Information Systems Agency, NIST, and representatives from the Army, Navy, and Marines. Over the course of the next 11 months, NIST made several updates to the content and posted the revised versions on its Web site. The first major version of the configuration settings, version 1.0, was posted on NIST's Web site in June 2008 after a period of public comment. Based on implementation information reported by the agencies to NIST in March 2008, agency feedback on settings that were problematic to implement, and comments from the federal community, OMB had NIST remove 40 settings from the original beta version for version 1.0.

In addition to publishing the FDCC settings, NIST also has responsibility for:

¹²According to agency-reported data, approximately 3.7 million workstations in use at the 24 federal agencies use either Windows XP or Windows Vista as the operating system.

¹³OMB Memorandum for Chief Information Officers, *Managing Security Risk By Using Common Security Configurations* (Washington, D.C.: Mar. 20, 2007); OMB, *Memorandum for the Heads of Departments and Agencies: Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, M-07-11 (Washington, D.C.: Mar. 22, 2007).

-
- Developing resources, in collaboration with Microsoft, to aid agencies in deploying and testing the security configuration settings within their computing environments. These include group policy objects,¹⁴ which allow agencies to deploy the settings to desktop and laptop computers agencywide, and virtual hard-disk files,¹⁵ which allow agencies to test the settings in a non-operational environment. These files were first made available for agencies to download from NIST's Web site starting in July 2007 and were later updated with the release of major version 1.0.
 - Establishing the Security Content Automation Protocol (SCAP),¹⁶ which can be used to support the automated checking, measuring, and monitoring of the FDCC settings for compliance. Product vendors can create a tool (i.e., application) that uses SCAP for these activities.
 - Validating SCAP tools to ensure that a tool uses the features and functionality available through SCAP. In order for a tool to receive validation, a vendor must first have the tool tested by 1 of 10 independent testing laboratories accredited under NIST's National Voluntary Laboratory Accreditation Program.¹⁷ The testing results are then sent by the laboratory to NIST for review. If the tool passes, NIST will validate the SCAP tool, which is valid for 1 calendar year.

¹⁴A group policy object is a collection of group policy settings that is used as part of Microsoft's Active Directory service. The service enables an administrator to define and make changes to various security and policy settings for groups of users and computers.

¹⁵A virtual hard disk holds a virtual machine or computer, which uses software to emulate a computer with a complete hardware system, on another computer. Virtual hard disks can be used to validate the effectiveness of the security configurations and test for compatibility issues with legacy applications in a simulated environment rather than on actual workstations.

¹⁶SCAP was developed by NIST in collaboration with the Departments of Defense and Homeland Security and Mitre Corp to provide a standardized approach to maintaining the security of enterprise systems. With the announcement of FDCC, SCAP was utilized to check the configuration settings on workstations. The FDCC SCAP content is hosted on the National Checklist Program Web site. The National Vulnerability database is also being expanded to host the SCAP component standards. See also NIST, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP) (Draft)*, Special Publication 800-117 (Gaithersburg, MD: May 2009).

¹⁷Under the NIST National Voluntary Laboratory Accreditation Program, NIST accredits independent laboratories to perform specific tests outlined in the SCAP Validation Program Derived Test Requirements document on SCAP tools seeking validation. NIST determines whether to validate a SCAP tool based on the test results provided by the laboratory. Laboratories are accredited based on requirements defined in NIST Handbook 150 and NIST Handbook 150-17.

-
- Making technical changes to the SCAP that support the FDCC settings, such as when new specifications are added, existing specifications are updated, or when a more efficient method is found to test a particular setting. NIST has released two additional major versions to make technical modifications to the SCAP: version 1.1 in October 2008 and version 1.2 in April 2009. NIST also publishes patch content updates based on Microsoft's patch releases.
 - Posting frequently asked questions on its Web site on behalf of OMB to answer agencies' questions about testing, deployment, reporting deviations, and use of SCAP tools for evaluation of compliance. The questions have also provided clarification of the settings requirements and their applicability to different types of computers, including contractor-owned or operated machines. These questions are revised on a periodic basis as needed and as determined by NIST.

FDCC Aims to Improve Agencies' Information Security and Reduce IT Operating Costs

In its March 2007 directives to agencies to implement FDCC, OMB established two goals for the initiative: improve information security and reduce overall information technology (IT) operating costs for agencies that use or plan to use Windows XP or Vista operating systems on their workstations.¹⁸ By implementing the initiative, OMB intended that agencies should be able to achieve the following objectives:

- **Provide a baseline level of security** through the use of standardized configuration settings that limit access privileges granted to users and other access controls, thereby controlling what a user may or may not do on his or her workstation. The settings create a baseline from which agencies may increase the level of security by making the settings more restrictive or by employing firewalls and intrusion detection systems along with other security devices and practices.
- **Reduce risk from security threats and vulnerabilities** by employing the use of standards that are more restrictive than the default settings of the manufacturer. For example, the required settings do not allow the installation of unauthorized software, which lowers the risk of introducing a virus or other malicious device along with the software.

¹⁸OMB Memorandum for Chief Information Officers, March 20, 2007; OMB, M-07-11 (Mar. 22, 2007).

-
- **Save time and resources** by requiring all FDCC workstations within an agency to use the same settings. This standardization also allows an agency's IT department to be more efficient in repairing computer problems.
 - **Improve system performance** by restricting the access privileges of administrators and users to only those necessary to perform their duties. This helps to limit downloading of unapproved software and information that could tie up system and help desk resources.
 - **Decrease operating costs** by using standard configuration settings that allow IT personnel to solve a workstation problem once and then replicate that solution for every workstation in the agency, saving labor and time.
 - **Ensure public confidence in the confidentiality, integrity, and availability of government information** by standardizing strong security settings across all federal agencies. This will help to protect federal systems from cyber attacks and may help to ensure the public's confidence that their personal information will not be compromised.

OMB Established Requirements for Agency Implementation of FDCC

In its initial memorandums and subsequent guidance, OMB identified several requirements with which agencies were directed to comply in order to implement FDCC. The following are the key FDCC requirements:

- **Submit a draft implementation plan to OMB by May 1, 2007.**¹⁹ Agencies were required to submit an implementation plan to OMB describing how they intended to (1) test configuration settings in a non-production environment to identify any adverse effects on system functionality; (2) implement the settings and automate monitoring and use; (3) restrict administration of these settings to authorized professionals; (4) ensure, by June 30, 2007, that new IT acquisitions include the settings and require IT providers to certify that their products operate effectively using the settings; (5) apply Microsoft patches available from the Department of Homeland Security when addressing new Windows XP or Vista vulnerabilities; (6) provide to NIST documentation of any deviations²⁰ from these settings and the rationale for the deviations; and (7) ensure the

¹⁹OMB Memorandum for Chief Information Officers, March 20, 2007.

²⁰A deviation occurs when the parameter for a particular setting is different from the approved or official parameter for the setting. A deviation can have more or less stringent parameters from that of the approved parameter.

settings are incorporated into agency capital planning and investment control processes.

- **Adopt the Windows XP and Vista security configuration settings by February 1, 2008.**²¹ Agencies were required to implement the FDCC configuration settings on all government-owned desktops and laptops that use Windows XP or Vista operating systems and the Internet Explorer 7 or Windows Firewall applications. This requirement was later clarified to include desktops and laptops that are owned or operated by a contractor on behalf of or for the federal government or that are integrated into a federal system. The requirement excludes servers, embedded computers, process control systems, specialized scientific or experimental systems, and similar systems using these operating systems.²²

FDCC major version 1.0 includes 674 configuration settings for Windows XP and Windows Vista systems, when bundled with Internet Explorer 7 and Windows Firewall. Examples of these settings include the following:

- Specifies the number of minutes a locked-out account remains locked out before it automatically unlocks.
- Specifies the minimum number of characters a password must have.
- Specifies whether or not the user is prompted for a password when the system resumes from sleep mode.
- Requires the use of Federal Information Processing Standards-compliant²³ algorithms for encryption, hashing, and signing.²⁴

²¹OMB, M-07-11 (Mar. 22, 2007).

²²NIST frequently asked questions posted on NIST's FDCC Web site, January 28, 2008; OMB Memorandum for Chief Information Officers, *Guidance on the Federal Desktop Core Configuration (FDCC)*, M-08-22 (Washington, D.C.: Aug. 11, 2008).

²³Federal Information Processing Standards are standards to be used by federal organizations that are developed and published by NIST as part of its mandates under 40 U.S.C. § 11331 and 15 U.S.C. § 278g-3, as amended by FISMA.

²⁴Encryption is used to provide basic data confidentiality and integrity for data by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. A cryptographic hash function computes (or hashes) a fixed-length message digest from an arbitrary-length message. A message digest may be considered as an "electronic fingerprint" of the original message. Signing with a digital signature is used to detect unauthorized modifications to data and to authenticate the identity of the signer.

-
- Shuts the system down immediately if it is unable to log security audits.²⁵
 - Creates a log when Windows firewall with advanced security allows an inbound connection. The log will detail why and when the connection was formed.
 - **Document deviations and have them approved by a designated accrediting authority.** Agencies were required to document deviations initially as part of their draft implementation plan efforts.²⁶ OMB later required agencies to report these deviations to NIST in March 2008.²⁷ OMB also later noted²⁸ that configuration setting deviations are to be approved by the department or agency accrediting authority.²⁹
 - **Acquire a SCAP tool and use it to monitor FDCC.** Agencies are required to acquire a NIST-validated SCAP tool³⁰ and to use these tools when monitoring the settings.³¹
 - **Ensure that new acquisitions include security configuration settings.** Agencies are required to ensure that new acquisitions include

²⁵ A log is a record of the events occurring within an organization's systems and networks. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Shutting down the system if it is unable to log a security event helps to ensure that an administrator will review the log and correct the problem in order to recover the system for the user.

²⁶ OMB Memorandum for Chief Information Officers, March 20, 2007.

²⁷ NIST Frequently Asked Questions posted on NIST's FDCC Web site, March 4, 2008; Chief Information Officers Council e-mail to chief information officers on behalf of OMB, March 24, 2008.

²⁸ OMB, M-08-22 (Aug. 11, 2008).

²⁹ A department or agency accrediting authority is a senior management official or executive with the authority to formally accept responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

³⁰ OMB Memorandum to Chief Information Officers, *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations* (Washington, D.C.: July 31, 2007).

³¹ OMB, M-08-22 (Aug. 11, 2008).

FDCC settings and products of information technology providers operate effectively using them.³²

- **Submit FDCC compliance reports to NIST by March 31, 2008.** Agencies were required to submit a spreadsheet that summarized workstation counts, setting deviations, and descriptions of plans of action and milestones³³ for the deviations, along with related reports generated by a SCAP tool for each operational environment present within the agency.³⁴
- **Report on status of FDCC compliance in annual FISMA reporting.** Agencies were required to report the status of compliance with FDCC as part of FISMA reporting for fiscal year 2008. This requirement included reporting on whether the configuration settings had been adopted and implemented, with deviations documented; whether language relating to the use of FDCC settings had been included in contracts; and whether all workstations had the security settings implemented.³⁵ Agency inspectors general were asked to assess agencies' compliance with the reporting requirements. For fiscal year 2009, agencies and agency inspectors general were required to report the status of compliance with specific requirements including whether deviations had been documented and language relating to the use of FDCC settings had been included in all contracts.³⁶

³²OMB Memorandum for Chief Information Officers and Chief Acquisition Officers, *Ensuring New Acquisitions Include Common Security Configurations*, M-07-18 (Washington, D.C.: June 1, 2007). In February 2008, the Federal Acquisition Regulation was revised to require agencies to use common security configurations, as appropriate. See 48 C.F.R. § 39.101(d) (73 FR 10967, 10968, Feb. 28, 2008).

³³Plans of action and milestones, also known as remedial action plans, can help agencies identify and assess security weaknesses in information systems such as deviations in system configurations, and set priorities and monitor progress in correcting them.

³⁴NIST Frequently Asked Questions posted on NIST's FDCC Web site, March 4, 2008; Chief Information Officers Council e-mail to chief information officers on behalf of OMB, March 24, 2008.

³⁵OMB, Memorandum for Heads of Executive Departments and Agencies, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-08-21 (Washington, D.C.: July 14, 2008).

³⁶OMB Memorandum for Heads of Executive Departments and Agencies, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, M-09-29 (Washington, D.C.: Aug. 20, 2009).

Agencies Have Not Fully Implemented FDCC Settings, but Most Have Complied with Other Requirements

None of the agencies has fully implemented all FDCC configuration settings on all applicable workstations, although most have complied with other requirements. Specifically, 11 agencies reported they had completed implementation of an agency-approved subset of the FDCC settings and do not plan to implement all the configuration settings, while the remaining agencies reported they are still completing implementation of the settings. However, most agencies have generally complied with other initiative requirements. For instance, 19 agencies have fully documented their deviations and 16 have established a policy for having those deviations approved by a designated authority. In addition, 15 agencies have acquired and deployed a NIST-validated SCAP tool to monitor the compliance of their setting implementation. Eight agencies have also incorporated language into their contracts to ensure that new acquisitions comply with FDCC.

Most Agencies Submitted FDCC Implementation Plans to OMB, but Did Not Address All Required Activities

While agencies were required to submit a draft implementation plan to OMB by May 1, 2007, fewer than half of the agencies developed plans that addressed the seven actions necessary to fully implement the initiative. Of the 24 agencies, 19 provided their plans to us, while 5 agencies either did not develop an implementation plan or were unable to locate a copy of the plan.³⁷ Of the 19 plans, 11 described how the agency intended to implement each of the seven actions required by OMB. The remaining 8 plans either did not address the actions or described only some of them. Table 1 shows how many agencies addressed each of the required actions in their FDCC implementation plans.

³⁷These 5 agencies were the Departments of Education, Energy, and Transportation; the Small Business Administration; and the Social Security Administration.

Table 1: Number of Agency FDCC Implementation Plans That Addressed Required Actions

Required action	Agency plans that addressed the action
1. Test configurations in a non-production environment to identify adverse effects on system functionality.	16
2. Implement the configurations and automate monitoring and use.	16
3. Restrict administration of these configurations to authorized professionals.	15
4. Ensure by June 30, 2007, that new acquisitions include the configurations and require information technology providers to certify that their products operate effectively using the configurations.	11
5. Apply Microsoft patches available from Department of Homeland Security when addressing new Windows XP or Vista vulnerabilities.	12
6. Provide NIST documentation of any deviations from these configurations and the rationale for the deviations.	15
7. Ensure these configurations are incorporated into agency capital planning and investment control processes.	12

Source: GAO analysis of agency FDCC implementation plans submitted to OMB.

Officials from one of the agencies whose plan did not address the required activities told us that OMB had provided feedback and requested changes to the plan, but the remaining agencies indicated that OMB had not provided feedback on the submitted plans and had not requested any changes. OMB was unable to confirm whether the 24 agencies had submitted the implementation plans by the required deadline because, officials stated, this information had been archived with the previous administration. As discussed later in the section on lessons learned, agencies experienced problems in implementing this requirement due to unrealistic deadlines.

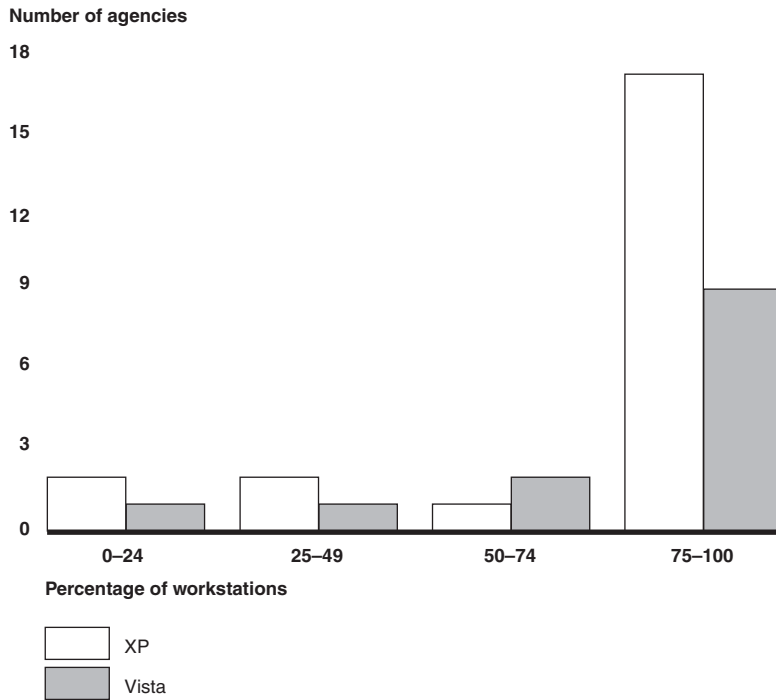
All Agencies Reported Implementing a Subset of FDCC Settings

Though agencies were required to adopt and implement the FDCC settings by February 1, 2008, as of September 2009, none of the 24 major agencies reported that they had adopted and fully implemented the complete set of prescribed settings on all applicable workstations. Instead, all agencies planned to implement a subset of the FDCC settings, which they referred to as their agency baseline; these baselines included deviations from the approved parameters established by FDCC, in some cases for up to one-

fifth of the settings.³⁸ As of September 2009, 11 agencies reported they had completed implementation of their baselines on all applicable workstations, and 11 were still in the process of finishing implementation of their baseline. The other 2 agencies were unable to provide sufficient data to determine the status of implementation because they either lacked a SCAP tool or had data reliability issues due to using multiple tools. (See app. II for more details on the status of each agency in implementing the FDCC settings, as of September 2009.) For those agencies that were still in the process of completing implementation of their baseline, agency officials reported various milestones for expected completion; however, some of those deadlines had not been met, and other agency officials did not report a milestone for completion. For example, a few agency officials indicated they would complete implementation by September 2009; however, this deadline was not met. Figure 1 summarizes the status of agency-reported implementation of their FDCC baselines for applicable workstations with Windows XP and Vista operating systems.

³⁸Agency implementation of FDCC may also not include implementation of Windows Firewall or Internet Explorer 7 settings if these applications are not being used by the agency.

Figure 1: Agency-Reported Implementation of FDCC Baseline as of September 2009



Source: GAO analysis of data reported by agencies in GAO data collection instrument.

Agency officials told us that several factors had influenced their decision to establish deviations, whether less or more stringent, from the settings. These factors included cases where FDCC settings

- had an adverse impact on applications, production, or legacy systems;
- conflicted with agency policy;
- prohibited agency administrators from completing tasks; and
- impaired the capability to provide customer support or remote assistance.

In establishing their baselines, agencies allowed a range of deviations, some with parameters that were less stringent (e.g., less secure) than the approved parameters, while others were more stringent. Of the 24 agencies, 23 provided us a list of their deviations and 1 agency indicated it had not developed a list. Each of the 23 lists identified deviations that were less stringent than the FDCC settings. Specifically, 15 agencies had 10 or more less-stringent deviations, and 6 agencies had 40 or more less-

stringent deviations, which is 6 percent of the 674 total number of FDCC settings. Table 2 shows the range of the number of less-stringent deviations and the corresponding number of agencies.

Table 2: Range of the Number of Less-Stringent Deviations with the Corresponding Number of Agencies

Range of deviations	Number of agencies
1-9	8
10-19	4
20-39	5
40-75	3
76-130	3

Source: GAO analysis of agency reported data.

Our analysis revealed ten most common less-stringent deviations across the federal government. For example, 21 of the 23 agencies that provided deviation lists had a deviation for the use of encryption algorithms³⁹ that are compliant with Federal Information Processing Standards, and 17 agencies had a deviation for the setting regarding digital signatures of client communications. Table 3 shows the 10 most common less-stringent deviations and the number of agencies that reported having them.

Table 3: Ten Most Common Less-Stringent FDCC Deviations at Federal Agencies

FDCC setting	Operating system	Number of agencies
Determines whether Federal Information Processing Standards-compliant encryption algorithms must be used.	XP/Vista	21
Determines whether the computer always digitally signs client communications.	XP/Vista	17
Determines what happens when an attempt is made to install a device driver that has not been certified by the Windows Hardware Quality Lab.	XP	16
Determines which password hashing algorithm is used for network logons.	XP/Vista	12

³⁹Encryption algorithms are mathematical processes used to transform plain text into cipher text for the purposes of encryption.

FDCC setting	Operating system	Number of agencies
Determines which users are allowed to use a network utility tool.	XP	12
Determines whether the Server Message Block server is required to perform packet signing.	XP/Vista	12
Determines who can connect to the workstation over the network.	XP/Vista	11
Determines the least number of characters that a password for a user account can contain.	XP/Vista	11
Determines whether a wireless configuration service can be used.	XP	10
Determines whether users can make remote assistance invitations for workstations.	XP/Vista	9

Source: GAO analysis of agency data.

Additionally, 7 agencies listed deviations that were more stringent (e.g., had parameters that were more secure) than the FDCC settings. Of the 7 agencies with more-stringent deviations, 1 had 10 or more of these more-stringent deviations, while the remaining 6 agencies had fewer than 10. There is also a common set of these more-stringent deviations among the 7 agencies. For example, 3 agencies have a deviation for duration accounts can be locked out, 2 agencies have a deviation for how many invalid logon attempts can occur before an account is locked out, and 2 agencies have a deviation for the type of user who can format and eject removable media.

Until those agencies that have not completed implementation of their FDCC baseline (see app. II) establish firm milestones for completion and complete implementation, agencies risk not achieving the potential benefits of the initiative.

Most Agencies Documented Deviations, but Eight Did Not Establish a Policy for Approving Them

Although OMB guidance indicates that agencies are to document and have a designated accrediting authority approve deviations from FDCC, several agencies did not do so. Of the 24 agencies, 23 had deviations and 1 did not maintain a list. Of the 23, 19 had fully documented their deviations but 4 had not. In addition, 16 agencies established a policy to have deviations approved by a designated accrediting authority, while 8 agencies have not established such a policy. Table 4 shows which agencies have documented deviations and have a policy in place to approve deviations by a designated authority.

Table 4: Status of Agency Compliance with Deviation Guidance

Agency	Documented deviations	Have policy to approve deviations by designated authority
Agriculture	No	No
Commerce	Yes	Yes
Defense	Yes	Yes
Education	Yes	Yes
Energy	No	Yes
Environmental Protection Agency	Yes	No
General Services Administration	Yes	Yes
Health and Human Services	Yes	Yes
Homeland Security	Yes	No
Housing and Urban Development	Yes	Yes
Interior	No ^a	No ^a
Justice	Yes	No
Labor	Yes	Yes
National Aeronautics and Space Administration	Yes	Yes
National Science Foundation	Yes	Yes
Nuclear Regulatory Commission	Yes	No
Office of Personnel Management	No	Yes
Small Business Administration	Yes	No
Social Security Administration	Yes	No
State	Yes	Yes
Transportation	Yes	Yes
Treasury	Yes	Yes
U.S. Agency for International Development	Yes	Yes
Veterans Affairs	Yes	Yes

Source: GAO analysis of agency documentation and responses by agency inspectors general to fiscal year 2009 FISMA reporting question.

^aAlthough the Department of the Interior documented deviations and had them approved by a designated authority at the department level, all of its agency components had not implemented these requirements.

Agency officials who had not documented deviations said they either did not maintain lists for field offices or had not yet completed the process for establishing the agency baseline and documenting the deviations. Officials from agencies that did not have a policy in place for approving deviations told us they were still working to develop an approval process. Until

agencies document their FDCC deviations or have a policy in place to approve those deviations, they cannot fully assess the potential risk of not implementing the required settings and they cannot ensure that configuration baselines are effectively controlled and maintained.

Six Agencies Have Yet to Acquire a SCAP Tool and Use It to Monitor FDCC Configurations

Agencies were required to obtain a NIST-validated SCAP tool and use it to consistently monitor the implementation of the configuration; however, while 15 agencies reported acquiring and deploying NIST-validated tools, 6 had not. Of the 3 remaining agencies, some of their components have a NIST-validated SCAP tool, while the other components either do not have a tool or do not use a NIST-validated tool for monitoring workstation configurations. Regardless of whether the tool has been validated or not, most agencies used one to monitor FDCC implementation. However, 2 agencies that had a validated tool had not yet established a policy for monitoring compliance. Table 5 shows which federal agencies have acquired a NIST-validated tool and were using it to monitor their workstation configurations.

Table 5: Status of Agency Acquisition and Use of a NIST-validated SCAP Tool

Agency	NIST-validated SCAP tool acquired and deployed	NIST-validated SCAP tool used to monitor compliance
Agriculture	Yes	Yes
Commerce	Partially	Partially
Defense	Yes	Yes
Education	Yes	Yes
Energy	Partially	Partially
Environmental Protection Agency	Yes	Yes
General Services Administration	Yes	Yes
Health and Human Services	Yes	No ^b
Homeland Security	Yes	No
Housing and Urban Development	No	No
Interior	Partially	Partially
Justice	No ^a	No ^c
Labor	Yes	Yes
National Aeronautics and Space Administration	Yes	Yes
National Science Foundation	No ^a	No ^c
Nuclear Regulatory Commission	Yes	Yes

Agency	NIST-validated SCAP tool acquired and deployed	NIST-validated SCAP tool used to monitor compliance
Office of Personnel Management	Yes	Yes
Small Business Administration	Yes	Yes
Social Security Administration	No ^a	No
State	Yes	Yes
Transportation	No ^a	No ^c
Treasury	Yes	Yes
U.S. Agency for International Development	Yes	Yes
Veterans Affairs	No	No

Source: GAO analysis of agency data.

^aAgency has acquired a NIST-validated tool but has not completed deployment at the agency.

^bAlthough the agency lacks a policy for monitoring compliance, it does perform scanning of its workstations using a NIST-validated SCAP tool.

^cAgency or components within the agency used a SCAP tool not currently validated by NIST to monitor compliance.

Note: Agency was given a rating of “partially” if some components had acquired a validated SCAP tool and used it to monitor compliance but other components had not.

At agencies that did not have a NIST-validated SCAP tool, officials told us they were in the process of acquiring a tool but had been delayed due to funding issues. For those agencies where only some components had acquired a tool, officials told us their components were responsible for acquiring a tool and noted that funding had been an issue. At agencies without a policy for monitoring implementation, officials told us that either a policy had not been finalized or a policy would be developed once a SCAP tool had been acquired. However, officials from one of these agencies noted that although they lacked a policy, they were still performing some monitoring of workstations. Until agencies acquire and deploy a NIST-validated SCAP tool and develop, document, and implement policies to monitor compliance, they will not be able to ensure that the FDCC settings have been successfully implemented to help protect the confidentiality, integrity, and availability of their information.

Most Agencies Have Not Incorporated Language into Contracts

Although OMB requires agencies to include language in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them, most agencies have not done so. Eight agencies had incorporated the language into their contracts, while 13 agencies had not, and 3 agencies had

partially implemented the requirement. Table 6 shows which agencies have incorporated language into their contracts.

Table 6: Agency Incorporation of Language into Contracts

Agency	Language incorporated
Agriculture	Yes
Commerce	No
Defense	No
Education	Yes
Energy	No
Environmental Protection Agency	Yes
General Services Administration	Yes
Health and Human Services	No
Homeland Security	No
Housing and Urban Development	No
Interior	Yes
Justice	No
Labor	Partially
National Aeronautics and Space Administration	Yes
National Science Foundation	Yes
Nuclear Regulatory Commission	Partially
Office of Personnel Management	No
Small Business Administration	No
Social Security Administration	No
State	Yes
Transportation	No
Treasury	Partially
U.S. Agency for International Development	No
Veterans Affairs	No

Source: GAO analysis and agency inspector general-provided responses for FISMA fiscal year 2009 reporting.

Note: Agencies were given a rating of “partially” if some components had incorporated the language into contracts but others had not, or if some contracts had the language incorporated, but others did not.

Officials from agencies that had not included language in the contracts had either included language in only a portion of the contracts reviewed, or the agency indicated it was still working on incorporating the language into its contracts. In addition, two agencies had one or more components that had not included the language in contracts. Until these agencies ensure that

language is included into contracts to ensure that new acquisitions include FDCC settings and products of information technology providers operate effectively using them, agencies will not be able to ensure that new acquisitions are in compliance with FDCC requirements.

Majority of Agencies Reported Status of Compliance with FDCC to NIST, but Many Indicated No Plans to Mitigate Deviations

Although most agencies submitted a compliance status report to NIST, the documentation was not always complete, including plans for mitigating deviations, or timely. Agencies were required to report to NIST the status of their compliance with FDCC by March 31, 2008, and submit a list of deviations, their plans of action and milestones for mitigating the deviations, and copies of reports generated by their SCAP tools. The majority of the agencies in our review submitted documentation to NIST; however, 2 agencies told us they had not submitted information to NIST, and 1 agency was unable to locate all the documents submitted. Of the 21 agencies that provided documentation, 12 agencies submitted all of the required information and documents. The remaining 9 agencies were either missing the required information or did not submit all of the required SCAP tool reports. In addition, while many of the agencies listed deviations, they either noted they did not plan to mitigate the deviations, or made general statements about addressing them at some point in the future. Furthermore, only 13 of the agencies in our review generally met the March 31, 2008, deadline for submission, while the remaining agencies took an additional month or more to provide documentation to NIST. As discussed later in the section on lessons learned, agencies experienced problems in implementing this requirement due to unrealistic deadlines.

Implementing FDCC Resulted in Benefits and Lessons Learned, but Agencies Continue to Face Challenges in Meeting Requirements

While implementation of FDCC can result in improvements to agencies' information security as well as other benefits, such as cost savings, attempting to meet the requirements yielded lessons learned that could improve the implementation of future versions of FDCC or other workstation configurations. In addition, agencies continue to face significant challenges in meeting FDCC requirements, monitoring their implementation of the settings, and measuring benefits of the initiative, among other things.

Implementing FDCC Can Enhance Security at Federal Agencies

FDCC has the potential both to increase agencies' information security and to standardize their management of workstations. Other potential benefits include cost savings arising from reduced power usage.

FDCC implementation enhances security by requiring stricter security settings on workstations than those that may have been previously in place at federal agencies. Specifically, some of the key configuration settings serve to secure agency workstations by restricting user and administrative rights to particular system functions. These settings reduce the potential for malware and other known vulnerabilities to affect agency workstations because the stricter access rights would prevent their automatic download and installation. As an example, officials at two agencies reported that FDCC was responsible for protecting their workstations from recent malicious code infections. The settings also reinforce access controls by restricting users' rights to what is necessary for their work. Ten of the agencies in our review attributed either increased security or increased security awareness to implementation of the settings and were generally supportive of a stricter configuration for the agency.

FDCC implementation also enabled agencies to reap the benefits of having more standardized configurations within agency computing environments. For example, a more secure enterprisewide Windows configuration and consistent workstation profile (i.e., the set of configuration settings and other software applied to a workstation) across the agency can not only improve security but can also make it easier to manage changes to the security features of workstation software, such as applying updates or patches. Updates or patches can be applied more expeditiously because there are fewer workstation profiles that they must be tested on, which also reduces the amount of necessary supporting documentation. Agency officials we spoke to confirmed that FDCC provided an improved understanding of their computing environment as well as a consistent desktop image across the department. Another official stated that adopting and implementing the configuration settings would raise awareness of the importance of workstation configuration management across the government.

Beyond the benefits to enhancing security within agency computing environments, there are other potential, if unanticipated, benefits to implementing particular settings and standardizing them across the federal government. For example, while settings related to activating and password-protecting screen savers can provide added security by locking the workstation while the user is not present, they could also reduce

power consumption and lead to savings in utility costs. One agency official said his agency was anticipating saving between \$10 million and \$15 million a year by implementing the power settings, and would be deploying a tool to track this data. In addition, an agency official from the Chief Information Officers Council's FDCC Change Control Board said the board was working on recommending what it considered "green settings" to OMB, which would also potentially reduce consumption of power and the paper used to print documents.⁴⁰ Officials at one agency also told us that because they had observed several benefits—including improved security, cost avoidance through acquisition of workstations with settings already implemented, and a simplification of the software development process—by implementing their agency FDCC baseline, they were in the process of developing or finalizing configuration settings for other operating systems and servers.

Lessons Learned

There are a number of lessons to be learned from the management and implementation of the FDCC initiative which, if considered, could improve the implementation of future versions of FDCC or other configuration efforts.

Having Realistic and Established Time Frames for Completion Is Needed to Ensure Successful Implementation

OMB did not provide a realistic time frame for agencies to meet the requirements of the initiative and complete implementation of FDCC by February 2008. This is due in large part to OMB not considering several constraints when establishing time frames for agencies to complete the requirements and implement the beta version of the settings within 7 months, including:

- Agencies were required to submit draft plans to implement the settings by May 1, 2007, approximately 3 months before being informed of the settings they were required to implement.
- Only one SCAP tool was validated in time for agencies to use to report the status of implementation to NIST, and one agency found that the tool did

⁴⁰The Chief Information Officers Council established an FDCC Change Control Board in June 2009 to make recommendations to OMB and NIST for changes to the FDCC settings. The board has established a yearly process during which it solicits suggestions for modifications to the settings from federal agencies, reviews the suggestions, and provides recommendations to NIST by July 1 of each year. The board plans to make its first recommendations on settings in July 2010.

not produce the needed reports required for NIST reporting. The earliest any of the other tools were validated was 7 months after the deadline.

- Multiple changes occurred to the FDCC content—including the settings, SCAP, and resources—that agencies were supposed to use in order to complete implementation by the February 2008 deadline. In addition, another version of the settings was released between the February deadline and the March 2008 compliance reporting deadline.

Furthermore, once the beta version of the settings was revised and major version 1.0 was released in June 2008, OMB did not establish a deadline for agencies to complete implementation of this version.

OMB officials confirmed they have not established a schedule for announcing changes to FDCC versions or implementation deadlines. However, they stated they were working with the Chief Information Officers Council and its newly developed FDCC Change Control Board to provide a framework for soliciting input and feedback on future versions of the settings on a yearly basis. Nevertheless, without realistic deadlines that are effectively communicated with sufficient notice, agencies will continue to face challenges in meeting implementation deadlines for future versions of FDCC.

Clarifying Guidance on Requirements for Deviations Is Necessary for Consistent Implementation

OMB and NIST guidance with regard to deviations was not always comprehensive, and agencies interpreted it in divergent ways. Specifically, OMB memorandums and guidance published on NIST's Web site were not clear as to

- under what conditions deviations were permitted;
- whether deviations could be permanent, or should be mitigated in a timely manner;
- how deviations should be documented, tracked, and approved by a designated authority; and
- how frequently and to whom deviations should be reported.

As a result, agencies interpreted this guidance in significantly different ways. Only one agency interpreted the requirements to mean that no deviations were permitted, while other agencies, by contrast, interpreted full implementation of FDCC to mean applying 85 to 95 percent of the settings, with deviations allowed under certain circumstances. In addition,

most agencies responded, either in their descriptions of plans of action and milestones or in interviews, that they had permanent deviations from FDCC, indicating they interpreted the guidance to mean that deviations could be permanent. However, several agencies also reported they may reduce the number of deviations as they upgrade, modify, or replace existing systems and applications.

In addition, agency processes to document and approve deviations varied. For example, some agencies documented and approved deviations at the agency level while other agencies allowed their components to determine the number of deviations and approve them. Some agency officials told us their list of deviations may not be complete because they provided deviations from only a few components, or did not track or maintain a list of deviations at the component level. For those agencies, officials noted they did not have visibility into the deviations documented and approved at the component level because responsibility for this was delegated to the components. Furthermore, agencies' interpretation of the requirement to report deviations to NIST varied, with some agencies stating they were only supposed to report deviations to NIST in March 2008, while other agencies said they reported deviations to NIST whenever they updated their lists.

OMB officials stated that full compliance with the configuration meant implementing all the settings without deviations on all applicable workstations, although they allowed agencies to document deviations and later required them to be approved. Nevertheless, without further clarification on the approval, permanence, and reporting of deviations, the federal government will continue to be hindered in consistently implementing FDCC, and OMB will be hindered in assessing the status and effectiveness of implementation across federal agencies.

Certain Testing Approaches Facilitated Successful Implementation

The variety of approaches agencies took to testing the settings prior to implementation affected how successful they were. In one case, an agency implemented the settings without testing, discovered problems, and subsequently changed its approach to include testing prior to implementation. Another agency reported having success with collaborative testing among agency components, which included officials from the components sharing results and other information at regular meetings. Officials from another agency stated that automated testing was a better approach because it allows for easier confirmation that there is a standard workstation configuration in use on the agency's systems. Ensuring that testing is carried out prior to implementation, with opportunities for information sharing and consideration of the benefits of

automation, can help agencies make implementation of future versions of FDCC or similar configurations more successful.

Phased Approach to Implementation Aided Successful Implementation

Agencies that implemented the settings in a phased, or sequential, fashion were able to avoid disruption in their operations and identify problems that arose during implementation. Officials from four agencies cited the benefits of or need for using such a phased implementation approach, rather than implementing the settings in one pass. One agency's officials observed that sequential implementation was key to avoiding system disruption and down time because settings were not applied to all components within the agency at the same time. Following such an approach for future versions of FDCC and other configurations could prove beneficial to agencies.

Further Collaboration between Agencies, OMB, and NIST Is Desired

Another success factor in implementing FDCC was frequent communication and collaboration among and within agencies. Officials from two agencies noted that collaboration among its agency components on testing was helpful in addressing problems that occurred. Agencies noted that keeping the lines of communication open, both among agency components and between OMB and NIST and other agencies, would help in making such an initiative more successful. One agency official recommended that there should be a way for NIST to communicate operational impacts prior to the release of new FDCC settings, and another suggested that future versions of FDCC should be vetted by the broader IT community before being rolled out to agencies. Officials from another agency stressed the importance of having communication and outreach among agencies to discuss FDCC issues and changes. Lastly, officials from one agency suggested having FDCC compliance sessions where agencies could discuss issues and learn from one another's experiences. Further collaboration between OMB, NIST, and agencies could increase the effectiveness of implementation among agencies and the chances for the success of similar future initiatives.

Independent Testing Provides an Important Perspective on Agency Compliance

Independent testing performed by the General Services Administration and Department of the Interior's Inspector General found compliance results that differed from agency-reported information. In a policy utilization assessment⁴¹ conducted over 2 years in multiple phases, the General Services Administration tested FDCC implementation at three agencies between December 2008 and February 2009. The results generally differed from agency-reported information on the level of policy implementation, level of compliance, and number of deviations reported between October 2008 and November 2008. At all three agencies, the scan results showed a higher level of policy implementation than the agencies had reported. In addition, two agencies learned they had a lower number of deviations on the workstation sample than they had reported, and two agencies were provided a more accurate indication of their level of compliance.

In September 2009, the Inspector General of the Department of the Interior reported widespread noncompliance with mandatory FDCC settings and noncompliance with agency directives at the agency.⁴² Based on testing performed during summer 2009, Interior averaged 68 percent compliance for the configuration settings, which varied from the compliance status reported to us. In addition, the Inspector General noted that agency components reported an additional 323 deviations at the components that were not documented and approved according to the agency's policy. The Inspector General made a recommendation to ensure Interior's compliance with FDCC guidance. These results suggest that agency self-reported compliance may not always be accurate and that continued independent testing can provide important insight into the extent of FDCC implementation. Additional independent testing performed by external parties could provide opportunities for agencies to acquire additional information to assist them in complying with FDCC requirements.

⁴¹The General Services Administration, under the direction of OMB, established the Policy Utilization Assessment Program in order to (1) conduct a series of implementation diagnostics to determine the extent and effectiveness of agency implementation and utilization of OMB information technology policies throughout the federal government; (2) establish an assessment methodology and best practices for use by individual agencies in improving policy implementation; and (3) document lessons learned and governmentwide trends to assist OMB in improving future information technology policy development efforts.

⁴²Office of the Inspector General, U.S. Department of the Interior, *Evaluation of Information Technology System Configuration*, ISD-EV-MOA-0003-2009 (Washington, D.C.: Sept. 23, 2009).

Advance Notice Can Aid in Allocating Limited Resources

In launching an initiative such as FDCC, having sufficient notice to marshal the necessary resources can improve agencies' chances of success. Agencies reported that having advance notice of the requirement to implement the initiative, with sufficient time for preparation and training, was necessary to successfully implement the initiative. Officials from one agency stated that such mandates should be widely announced well in advance of anticipated completion dates to allow all agencies appropriate lead time to ensure that budgets and resources would be available and that requirements and resulting impacts could be completely assessed. Further, agencies commonly reported a lack of sufficient resources (time, money, labor, technical expertise) to implement the FDCC settings, understand how the settings would affect their environments, address issues found with testing, and purchase a SCAP tool. Some agencies cited having to reallocate approved funding to cover the costs of implementation and the purchase of the tools. Although most agencies could not provide estimates of the time and labor spent implementing FDCC, several agencies provided estimates of the costs of implementation and purchasing SCAP tools, which ranged from the tens of thousands to hundreds of thousands of dollars. In addition, officials from a few agencies stated they did not always have staff dedicated specifically to FDCC, which contributed to delayed implementation. Ensuring sufficient lead time can help agencies better plan use of their resources to implement initiatives like FDCC.

Challenges Exist for Agencies in Fully Complying with FDCC Requirements

Agencies face several ongoing challenges to fully complying with FDCC requirements, including retrofitting their existing applications and systems to comply with the settings, assessing the risks associated with deviations, and monitoring workstations to ensure that the settings are applied and functioning properly.

Retrofitting Applications and Legacy Systems to Comply with Configuration Settings in Complex Agency Environments

Applying the configuration settings has and will continue to cause problems for agencies due to the variety of applications, legacy systems, and agency environments that exist within the federal government. In particular, agencies have legacy systems or applications that use old software that have to be reconfigured to work with the settings. In addition, while some agency environments consist of a small number of offices with under 10 thousand workstations, other agency environments have multiple components with hundreds of thousands of workstations that are spread out geographically across the country, and in a few cases, the world. Although agencies were required to implement all the FDCC settings, the number and scope of the deviations that agencies had to implement highlight the magnitude of the challenge that agencies faced in

implementing the settings. Agency officials confirmed during interviews that there were several challenges in retrofitting their systems and applications to comply with the settings, including the following examples:

- Some of the settings had affected other settings on workstations and servers, and it had been a challenge to determine which FDCC settings were responsible.
- Some of the settings impaired the functioning of custom programs, caused problems in environments, or interfered with basic functions (e.g., network printing).
- The settings prevented the agencies from accessing legitimate Web sites, such as certain federal, state, and local government sites.
- Applying particular FDCC settings to legacy systems or applications would require agencies to update their applications or operating systems.

However, potential solutions to these challenges are either not simple or may not exist. As new versions of the settings or other configurations are established, it will be important for OMB to recognize that retrofitting systems and applications to comply with new settings in complex environments will remain an ongoing challenge for agencies, and that sufficient time for implementation and the use of deviations may be necessary. However, OMB has not provided guidance to agencies on submitting plans for mitigating deviations, including the resources necessary for doing so. Until OMB provides guidance to agencies on submitting plans of actions and milestones for mitigating deviations, to include resources necessary for doing so, OMB will lack sufficient information to make decisions about the use of deviations and whether potential changes to FDCC are warranted.

Assessing the Risks Associated with Deviations

A related challenge for agencies is sufficiently assessing the risks associated with deviations from the official FDCC settings. As mentioned earlier, all agencies in our review had deviations, regardless of whether these deviations had been sufficiently documented or approved. There are risks associated with deviations from individual settings and groups of settings, not only at individual agencies but among agencies, depending on the agency's computing environment. For instance, having deviations such as passwords with a minimal number of characters, combined with allowing multiple users to connect to the workstation over the network and enabling wireless communication on the workstation, increases the risk that unauthorized users could gain access to workstations and

sensitive government information. However, many of the agencies in our review did not describe a process for assessing the combined risk of the deviations they had in place because deviations were submitted for approval on an individual basis, were submitted as part of a configuration that included other settings beyond FDCC, or, particularly at agencies where deviation approval was left up to components, the agency did not track the deviations at the component level.

Although OMB required agencies to approve deviations, it did not specify any guidance for agencies to use to consider the risks of having these deviations prior to approval. Until OMB specifies guidance for agencies to use to assess the risks of having deviations prior to approving them, including the combined risk of deviations in place across the agency, workstations may remain particularly vulnerable to cyber threats.

Consistent and Comprehensive
Monitoring of FDCC
Implementation on Agency
Workstations

Challenges also exist in effectively and consistently monitoring the implementation of FDCC in order to ensure the settings have been implemented properly and are continuing to function as intended. Specifically, the frequency and scope with which agencies scan workstations for compliance may not be sufficient to ensure the settings are working properly, and the results could potentially be incomplete or inconsistent. While some agencies scanned workstations on a weekly or bi-weekly basis, other agencies performed scans only when new patches or system updates had been installed or performed scanning only on a quarterly or annual basis. The infrequent monitoring on the part of some agencies could be due to the SCAP tool used: agency officials without an enterprisewide tool noted that frequent monitoring was impractical because regularly scanning each workstation required them to individually scan up to tens of thousands of workstations.

In addition, while some agencies scanned every workstation on their network, other agencies only performed scans on test workstations, which could be insufficient if agency workstation configurations do not match the tested workstations. Scans of workstations on agency networks may also be incomplete in cases where user populations work remotely or have contractor-owned workstations. Agencies that use a SCAP tool to scan all workstations connected to their network may miss workstations belonging to these populations, which might not be connected to the network depending on the time of the scan. Consequently, agencies may be relying on incomplete information on whether the settings are working as intended.

Having Sufficient Tools to Perform Monitoring of Workstations

While OMB guidance indicates that agencies should monitor compliance using SCAP, the guidance does not specify the frequency or scope in which monitoring should be performed. Until OMB improves its guidance on monitoring compliance using SCAP to include information on the frequency and scope with which agencies should perform monitoring, agencies may not be scanning with sufficient rigor to ensure the settings have been successfully implemented and are working properly.

Agencies did not always have sufficient tools to monitor implementation and compliance with FDCC. In particular, issues with the current NIST-validated SCAP tools include the following:

- Some tools generate errors when scanning for particular settings.
- Certain settings have to be checked manually because the tools do not scan for all settings.
- Some tools record false positives, particularly if the agency's parameter for a particular setting is stricter than the FDCC parameter.
- It takes time for vendors to update their SCAP tools after NIST changes SCAP content to address problems, with the result that the tools perform scans based on incorrect content.

Agency officials we interviewed confirmed there were issues with the SCAP tools, and many agencies and their components found it easier to use some combination of NIST-validated SCAP tools, group policy objects, or other configuration management software to monitor their configurations. In addition, several agencies indicated they had acquired or were in the process of acquiring a different SCAP tool that would provide better functionality and capabilities in order to meet their needs.

NIST officials confirmed they were aware of the issues with SCAP tools and stated they are taking steps to address them. For instance, NIST intends to release new requirements that SCAP tools must meet as well as change validation requirements so that vendors will be required to have their tools tested and validated against the new requirements within 1 year of the requirements being released. NIST requested comments on a draft of this document through January 2010, but hasn't released a final version. Once NIST releases the new requirements for SCAP tools and these tools are validated against these requirements, agencies should have more sufficient tools for monitoring implementation of FDCC.

Measuring Benefits of the Initiative

Although agencies have anecdotally reported a variety of benefits from efforts to implement FDCC, OMB and agencies face challenges in accurately assessing the impact and measuring the benefits of the initiative. This is because neither OMB nor the agencies have developed specific metrics to measure the effectiveness and program impact of the initiative. Specifically, they have not required or collected measures or metrics that address how effectively the initiative is mitigating security risks or reducing costs, two of its stated goals. For example, an official at one agency noted several benefits of implementing FDCC—a more secure user environment because of reduced user permissions, a stable development platform that resulted in cost savings and a simplification of the software development process, and a reduction in the number of customer support help calls and service calls by technicians. However, the official admitted that he did not have specific metrics for quantitatively measuring these benefits.

Implementing metrics that assess the effectiveness and program impact could give a more complete picture of the benefits of FDCC and help determine whether future versions of the settings or configurations for other operating systems or servers should be instituted. In our September 2009 report, we recommended that OMB, among other things, direct federal agencies to use balanced sets of information security measures that include effectiveness and impact, as well as compliance, and to require agencies to report on such a balanced set of measures.⁴³ Without performance measures and guidance to agencies for reporting the benefits of FDCC, OMB and federal agencies will be limited in their ability to determine if the initiative is meeting its goals of improving federal information security and reducing operating costs and if the initiative should be continued or expanded.

Conclusions

While agencies have taken steps toward implementing FDCC, work remains to be done in order to meet all the requirements established by OMB. Specifically, many agencies have applied an agency-defined subset of the configuration settings to their Windows workstations; however, none of the 24 major agencies has fully applied all the FDCC settings. Further, not all agencies have put a process in place for documenting or approving deviations from the FDCC baseline and have not yet acquired

⁴³GAO, *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, GAO-09-617 (Washington, D.C.: Sept. 14, 2009).

the required SCAP tool to monitor compliance with the settings. Unless agencies fulfill these requirements, OMB will not be able to ensure the effectiveness of the initiative.

The FDCC initiative was an innovative approach by OMB to standardize and thereby strengthen information security at federal agencies, but lessons learned indicate ways that implementation could have been more successful. Specifically, OMB did not establish realistic time frames for completion or provide comprehensive guidance on FDCC deviations, which has impacted agencies' ability to successfully implement the initiative. In addition, collaboration among OMB, NIST, and the agencies, as well as independent testing of FDCC implementation by external parties, may help agencies be more successful in their implementation efforts.

Finally, there are several ongoing challenges facing agencies in fully complying with the requirements, including retrofitting systems and applications amid complex environments, assessing the risks associated with deviations across each agency, and monitoring workstations to ensure the settings are applied and functioning properly. As OMB establishes additional versions of FDCC settings—or configuration settings for other applications or operating systems—understanding the lessons learned from implementation as well as the ongoing challenges agencies face will be essential to the initiative's success in ensuring public confidence in the confidentiality, integrity, and availability of government information.

Recommendations for Executive Action

To improve implementation of FDCC at federal agencies, we recommend that the Director of OMB take the following six actions:

- When announcing new FDCC versions, such as Windows 7, and changes to existing versions, include clear, realistic, and effectively communicated deadlines for completing implementation.
- Clarify OMB policy regarding FDCC deviations to include: whether deviations can be permanent or should be mitigated in a timely manner; requirements for plans of actions and milestones for mitigating deviations, including resources necessary for doing so; guidance to use for assessing the risk of deviations across the agency; and how frequently and to whom deviations should be reported to assist in making decisions regarding future versions.

-
- Inform agencies of the various approaches for testing the settings and implementing the initiative in phases, which may aid successful implementation.
 - Assess the efficacy of, and take steps to apply as appropriate, other lessons learned during the initial implementation of this initiative such as the need for (1) additional collaboration efforts, (2) independent testing, and (3) advance notice of requirements, to assist agencies in implementing this initiative.
 - Provide guidance on using SCAP tools to include information on the frequency and scope with which agencies should perform monitoring.
 - Develop performance measures and provide guidance to agencies for reporting the benefits of FDCC.

We are also making 56 recommendations to 22 of the 24 departments and agencies in our review to improve their implementation of FDCC requirements that were not being met. Appendix III contains these recommendations.

Agency Comments and Our Evaluation

In providing e-mail comments on a draft of this report, the lead IT policy analyst from OMB's Office of E-Government and Information Technology stated that OMB concurred with the report's findings, conclusions, and 6 recommendations addressed to OMB.

We also sent a draft of this report to the 24 agencies in our review and received written, e-mail, and/or oral responses from all 24 agencies. Of the 22 agencies to which we made recommendations, 14 (Agriculture, Defense, Environmental Protection Agency, General Services Administration, Health and Human Services, Justice, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, Treasury, U.S. Agency for International Development, and Veterans Affairs) generally agreed with our recommendations. One agency (Commerce) did not comment specifically on our recommendations and the remaining 7 agencies generally concurred with some of our recommendations but provided qualifying comments with others. The agencies' comments and our responses are summarized below:

- In oral comments on a draft of the report, the Department of Energy's Acting Associate Chief Information Officer for Cyber Security generally

concluded with 4 of our 5 recommendations. However, he requested that our recommendations to ensure that all components acquire and deploy a NIST-validated SCAP tool, and develop, document, and implement a policy to monitor compliance using a NIST-validated tool be clarified to pertain only to those components that were required to implement FDCC. We agree that this modification clarifies the intent of our recommendations and have modified those recommendations as appropriate. Further, in commenting on our fifth recommendation to ensure that FDCC acquisition language was included in contracts, the Acting Associate Chief Information Officer for Cyber Security stated that the department will continue to evaluate our recommendation and determine an appropriate implementation approach.

- In written comments on a draft of the report, the Department of Homeland Security's Chief Information Officer concurred with 3 of our 4 recommendations. He also concurred, with a caveat, with our fourth recommendation to ensure that FDCC acquisition language was included in contracts. The Chief Information Officer stated that the department already has regulations in place to ensure new acquisitions meet FDCC requirements. We agree that the department has regulations in place. However, as indicated in our report, the FDCC acquisition language had not been incorporated into all contracts. The Department of Homeland Security's comments are reprinted in appendix VIII.
- In written and oral comments on a draft of the report, the Department of Housing and Urban Development's Chief Information Officer generally concurred with 3 of our 4 recommendations. In written comments on our recommendation that the department ensure FDCC acquisition language is included in contracts, he stated that the department had a policy in place for including clauses in contracts. After subsequent discussion with department representatives, they orally concurred with our recommendation. In written comments on our recommendation that the department develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority, the Chief Information Officer stated that the department had provided us with a copy of its policy for approving deviations in December 2009. After reviewing additional documentation provided, we agree that the department had met the requirement, modified the report as appropriate, and removed the recommendation. The Department of Housing and Urban Development's comments are reprinted in appendix IX.
- In written comments on a draft of the report, the Department of the Interior's Assistant Secretary for Policy, Management, and Budget concurred with our recommendations, subject to modifications that

reduced redundancy in the recommendations and clarified that components should follow the department's policy related to documenting and approving deviations, and acquiring and deploying NIST-validated tools to monitor compliance with FDCC. We agree that the suggested modifications clarified the intent of our recommendations, and have modified the recommendations accordingly. The Department of the Interior's comments are reprinted in appendix X.

- In written and oral comments on a draft of the report, the Department of Labor's Assistant Secretary for Administration and Management generally concurred with 1 of our 2 recommendations, subject to modification that clarified that FDCC acquisition language had been included in some contracts but not in all. After reviewing additional documentation provided, we modified the recommendation as appropriate. In written comments on our recommendation that the department complete deployment of a NIST-validated SCAP tool, the Assistant Secretary for Administration and Management stated that deployment of the tool had been completed prior to the end of our audit field work. After reviewing additional documentation provided, we agree that the department had met the requirement, modified the report as appropriate, and removed the recommendation. The Department of Labor's comments are reprinted in appendix XI.
- In written and oral comments on a draft of the report, the Office of Personnel Management's Chief Information Officer generally concurred with 3 of our 4 recommendations. In written comments on our recommendation on documenting deviations and having them approved by a designated authority, he said that the department has documented its deviations and approved them. After subsequent discussion with department representatives, they orally concurred with our recommendation. In addition, in written comments on our recommendation to develop, document, and implement a policy to approve deviations to FDCC by a designated authority, the Chief Information Officer stated that the agency has a policy in place. After reviewing documentation provided, we agree that the department had met the requirement, modified the report as appropriate, and removed the recommendation. The Office of Personnel Management's comments are reprinted in appendix XIII.
- In e-mail and oral comments on a draft of the report, the Department of Transportation's Chief Information Security Officer generally concurred with our 2 recommendations, subject to modification that clarified that the department had acquired a validated tool and was in the process of fully deploying it. After reviewing additional documentation provided, we

modified table 5 in the report to include a table footnote indicating a tool had been acquired but not deployed and revised the recommendation as appropriate. In addition, in e-mail comments on our recommendation to ensure that FDCC acquisition language is included in contracts, the Chief Information Security Officer stated that the department had provided a copy of the policy guidance on contract clauses to us. After subsequent discussion with department representatives, they orally concurred with our recommendation.

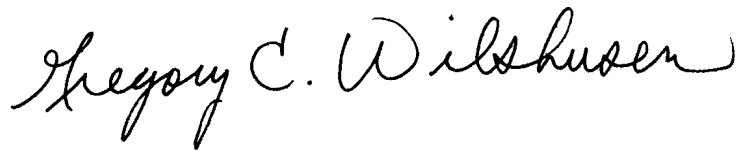
In addition, several agencies also provided technical comments, including one of two agencies to which we did not make recommendations. We have incorporated these comments as appropriate. The remaining agency to which we did not make recommendations stated that it did not have any comments.

Furthermore, for appropriate coverage of a federal-wide information technology contract issue, the Department of Defense suggested we add a recommendation that contract language be included in the Federal Acquisition Regulation "to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them." However, it was not within the scope of our review to evaluate whether such standard contract language was necessary or what it would entail. Nonetheless, the Department of Defense may wish to pursue this suggestion with OMB and other stakeholders for possible promulgation of a Federal Acquisition Regulation rule that would serve as a governmentwide template in solicitations or contracts for ensuring that FDCC settings are effectively incorporated and applied.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to other interested congressional committees, secretaries of the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Attorney General; the administrators of the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, Small Business Administration, and U.S. Agency for International Development; the commissioner of the Social Security Administration; the chairman of the Nuclear Regulatory Commission; and the directors of the National Science Foundation, Office of Management

and Budget, and Office of Personnel Management. The report also is available at no charge on the GAO Web site at <http://www.gao.gov>.

If you or your staff have any questions regarding this report, please contact me at (202) 512-6244 or at wilshuseng@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix XVIII.

A handwritten signature in black ink that reads "Gregory C. Wilshusen". The signature is written in a cursive, flowing style.

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

Relative to the 24 major federal agencies covered by the Chief Financial Officers Act, the objectives of our review were to (1) identify the goals, objectives, and requirements for the initiative; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiative; and (3) identify the benefits, challenges, and lessons learned in implementing this initiative.

To address our first objective, we reviewed applicable policies and memorandums issued by the Office of Management and Budget (OMB) and plans, artifacts, and other documentation provided by the National Institute of Standards and Technology (NIST). We also reviewed guidance and Federal Desktop Core Configuration (FDCC) and Security Content Automation Protocol (SCAP) materials located on NIST's Web site. In addition, we held discussions with OMB and NIST representatives to further assess the initiative's requirements and confirm that the material posted on their Web sites that we considered was current and accurate.

To address our second and third objectives, we obtained and analyzed policies, plans, artifacts, status reports, and other documentation relative to the requirements of the initiative from each of the 24 federal agencies in our review. We obtained information through interviews with officials from each of the 24 agencies, industry officials, security experts, officials from General Services Administration's Policy Utilization Assessment Program, and members of the Chief Information Officers Council and FDCC Change Control Board. We also met with staff from all 24 Offices of the Inspector General regarding their FDCC audit work performed as part of Federal Information Security Management Act fiscal year 2008 and 2009 reporting to obtain information on their audit methodology, findings, and related documentation. Based on our review of the adequacy of work performed, we have sufficient assurance to rely on work completed by the inspectors general in the context of our audit objective related to whether the agency had documented deviations and had incorporated language related to the use of FDCC settings into its contracts. We also analyzed the information we obtained from all sources to determine the benefits, challenges, and lessons learned from implementation of FDCC.

For our second objective, in order to determine the status of FDCC implementation at federal agencies, we developed a data collection instrument to obtain information on the number of workstations that had FDCC settings applied, either with no deviations or with deviations established at these agencies. To develop our data collection instrument, we reviewed the requirements of the initiative as well as the results from a previous data collection instrument used by NIST to collect status

information on FDCC as of March 2008. We designed the draft collection instrument in close collaboration with subject matter experts and participated in refining subsequent drafts of the instrument. We sent the data collection instrument to the officials at the Office of Chief Information Officer at the 24 federal agencies and asked the agencies to provide status information as of June 30, 2009, and as of September 30, 2009.

We e-mailed our first data collection instrument, to collect FDCC status data as of June 30, 2009, to all 24 agencies in early June 2009. When our collection ended in July 2009, we had received 19 usable responses. After examining the results from this data collection to identify inconsistencies and other indications of error, we concluded that the extent of response error and the overall low level of participation precluded the use of these data in our report.

To refine the data collection instrument to collect September 2009 data, we conducted pretests with officials from 3 agencies to clarify any ambiguous or potentially biased questions. These pretests were conducted by telephone with the 3 agencies, which were chosen to represent the variety of characteristics across the 24 agencies we would survey. These characteristics included the operating system used, type of workstation, composition and size of the agency, and method used to collect status information.

We sent this instrument to agency officials in mid-September 2009. We conducted follow-up contacts by e-mail and phone to encourage response and clarify individual answers. We received usable responses from 22 agencies, and ended the data collection period in November 2009. While our evaluation of the instrument data indicates that it is usable for the purposes of this report, the information may not be complete due to the inability of some agencies to provide information in the categories we requested, including some of the data supporting our estimates of contractor-owned workstations with FDCC compliance, and possibly some other estimates.

We conducted this performance audit from December 2008 to March 2010 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Percentage of Agency Workstations with FDCC Settings Implemented as of September 2009

The table below shows, for the 24 agencies from which we collected data using our data collection instrument, the percentage of applicable Windows XP and Vista workstations that have all FDCC settings implemented with no deviations, workstations with an agency baseline implemented and deviations documented, and workstations that do not have the settings implemented.

Table 7: Agency-Reported Percentages of Workstations with FDCC Settings Implemented as of September 2009

Agency	Platform	Implemented without deviations	Implemented with deviations (agency baseline)	Not implemented
Agriculture	XP	8%	0%	92%
	Vista	0	0	100
Commerce	XP	9	91	0
	Vista	23	77	0
Defense	XP	0	96	4
	Vista	99	0 ^a	1
Education	XP	0	100	0
	Vista	0	100	0
Energy	XP	Unknown	72	Unknown
	Vista	Unknown	71	Unknown
Environmental Protection Agency	XP	Unknown	Unknown	Unknown
	Vista	Unknown	Unknown	Unknown
General Services Administration	XP	0	84	16
	Vista	Not applicable	Not applicable	Not applicable
Health and Human Services	XP	0	99	1
	Vista	0	94	6
Homeland Security	XP	0	5	95
	Vista	0	29	71
Housing and Urban Development	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
Interior	XP	1	48	51
	Vista	69	18	13
Justice	XP	3	96	1
	Vista	0	100	0
Labor	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
National Aeronautics and Space Administration	XP	Unknown	87	Unknown
	Vista	Unknown	52	Unknown

Appendix II: Percentage of Agency Workstations with FDCC Settings Implemented as of September 2009

Agency	Platform	Implemented without deviations	Implemented with deviations (agency baseline)	Not implemented
National Science Foundation	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
Nuclear Regulatory Commission	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
Office of Personnel Management	XP	1	40	59
	Vista	Not applicable	Not applicable	Not applicable
Small Business Administration	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
Social Security Administration	XP	0	100	0
	Vista	0	100	0
State	XP	0	100	0
	Vista	0	100	0
Transportation	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
Treasury	XP	0	99	1
	Vista	0	99	1
U.S. Agency for International Development	XP	0	100	0
	Vista	Not applicable	Not applicable	Not applicable
Veterans Affairs	XP	Unknown	Unknown	Unknown
	Vista	Unknown	Unknown	Unknown

Source: GAO analysis of data reported by agencies in GAO data collection instrument.

Note: Percentages in the table have been rounded. Both the number of government-owned and contractor-owned workstations were included in agency totals if the number of contractor-owned workstations was not separated from the number of government-owned workstations that was provided by the agency. Agencies that did not have Vista workstations were listed as not applicable. An agency that was unable to provide sufficient data to determine the status of implementation was listed as unknown.

*Agency reported having no deviations for the implementation of the settings on this operating system.

Appendix III: Recommendations to Departments and Agencies

Agriculture

To improve the department's implementation of FDCC, we recommend that the Secretary of Agriculture take the following three actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- document deviations to FDCC and have them approved by a designated accrediting authority; and
- develop, document, and implement a policy to approve deviations by a designated accrediting authority.

Commerce

To improve the department's implementation of FDCC, we recommend that the Secretary of Commerce take the following three actions:

- ensure all components have acquired and deployed a NIST-validated SCAP tool to monitor compliance with FDCC;
- ensure all components develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Defense

To improve the department's implementation of FDCC, we recommend that the Secretary of Defense take the following two actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion, and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Energy

To improve the department's implementation of FDCC, we recommend that the Secretary of Energy take the following five actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;

- document deviations to FDCC and have them approved by a designated accrediting authority;
- ensure all components that are required to implement FDCC have acquired and deployed a NIST-validated SCAP tool to monitor compliance with FDCC;
- ensure all components that are required to implement FDCC develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts of those components that are required to implement FDCC to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

**Environmental Protection
Agency**

To improve the agency's implementation of FDCC, we recommend that the Administrator of the Environmental Protection Agency take the following two actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion, and
- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority.

**General Services
Administration**

To improve the agency's implementation of FDCC, we recommend that the Administrator of the General Services Administration take the following action:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion.

**Health and Human
Services**

To improve the department's implementation of FDCC, we recommend that the Secretary of Health and Human Services take the following three actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;

- develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Homeland Security

To improve the department's implementation of FDCC, we recommend that the Secretary of Homeland Security take the following four actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority;
- develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Housing and Urban Development

To improve the department's implementation of FDCC, we recommend that the Secretary of Housing and Urban Development take the following three actions:

- acquire and deploy a NIST-validated SCAP tool to monitor compliance with FDCC;
- develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Interior

To improve the department's implementation of FDCC, we recommend that the Secretary of the Interior take the following three actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- ensure all components implement the department's existing policy to document deviations to FDCC and have those deviations approved by a designated accrediting authority; and
- ensure all components implement the department's existing policy to acquire and deploy a NIST-validated SCAP tool and monitor compliance with FDCC.

Justice

To improve the department's implementation of FDCC, we recommend that the Attorney General take the following four actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority;
- complete deployment of a NIST-validated SCAP tool to monitor FDCC compliance; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Labor

To improve the department's implementation of FDCC, we recommend that the Secretary of Labor take the following action:

- complete efforts to ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

**National Aeronautics and
Space Administration**

To improve the agency's implementation of FDCC, we recommend that the Administrator of the National Aeronautics and Space Administration take the following action:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion.

National Science
Foundation

To improve the agency's implementation of FDCC, we recommend that the Director of the National Science Foundation take the following action:

- complete deployment of a NIST-validated SCAP tool to monitor FDCC compliance.

Nuclear Regulatory
Commission

To improve the agency's implementation of FDCC, we recommend that the Chairman of the Nuclear Regulatory Commission take the following two actions:

- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority, and
- ensure that all components include language in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Office of Personnel
Management

To improve the agency's implementation of FDCC, we recommend that the Director of the Office of Personnel Management take the following three actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- document deviations to FDCC and have them approved by a designated accrediting authority; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Small Business
Administration

To improve the agency's implementation of FDCC, we recommend that the Administrator of the Small Business Administration take the following two actions:

- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority, and

- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Social Security
Administration

To improve the agency's implementation of FDCC, we recommend that the Commissioner of the Social Security Administration take the following four actions:

- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority;
- complete deployment of a NIST-validated SCAP tool to monitor compliance with FDCC;
- develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Transportation

To improve the department's implementation of FDCC, we recommend that the Secretary of Transportation take the following two actions:

- complete deployment of a NIST-validated SCAP tool to monitor compliance with FDCC, and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Treasury

To improve the department's implementation of FDCC, we recommend that the Secretary of the Treasury take the following two actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion, and
- ensure that all components include language in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

U.S. Agency for
International Development

To improve the agency's implementation of FDCC, we recommend that the Administrator of the U.S. Agency for International Development take the following action:

- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Veterans Affairs

To improve the department's implementation of FDCC, we recommend that the Secretary of Veterans Affairs take the following four actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- acquire and deploy a NIST-validated SCAP tool to monitor compliance with FDCC;
- develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool; and
- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.


Appendix IV: Comments from the U.S. Department of Agriculture



United States
Department of
Agriculture

Office of the Chief
Information Officer
1400 Independence
Avenue SW
Washington, DC
20250

TO: Gregory Wilshusen
Director
Information Security Issues
Government Accountability Office

FROM: Christopher L. Smith 
Chief Information Officer
Office of the Chief Information Officer

SUBJECT: USDA Comments on Draft Report GAO-10-202

The United States Department of Agriculture (USDA) is pleased with the opportunity to review and comment on the draft GAO report Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements (GAO-10-202).

USDA agrees with and accepts the findings of the draft Report, as they pertain to USDA. The draft Report recommends that the Secretary of Agriculture take the following three actions:

- complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;
- document deviations to FDCC and have them approved by a designated accrediting authority (DAA); and
- develop, document, and implement a policy to approve deviations by a designated accrediting authority.

We support GAO's call for further clarification from OMB on the governmentwide standards for documenting deviations from the FDCC and would be pleased to work with OMB, NIST and other departments and agencies to further that end.

Appendix V: Comments from the Department of Commerce

Note: GAO comment supplementing those in the report text appear at the end of this appendix.



THE SECRETARY OF COMMERCE
Washington, D.C. 20230

February 18, 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:


Thank you for the opportunity to review the General Accountability Office's (GAO) draft report, "Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements" (GAO-10-202).

We concur that this report is a reasonable assessment of the current Federal Desktop Core Configuration (FDCC) situation among federal agencies. The Department of Commerce (Department) offers the following comments regarding the GAO's conclusions.

- As noted in GAO-10-202, there remain some technically problematic FDCC settings for many agencies and, as such, there may be some scenarios where risk should be accepted
- FDCC applicability has been clarified by the National Telecommunications and Information Administration's guidance; however, it has not been officially issued in an updated memorandum from the Office of Management and Budget (OMB)
- There is not clear guidance from OMB in regard to FDCC deviations and how these deviations are documented by federal agencies; the FDCC deviations are an operational necessity in some cases.
- Collaboration on future secure configuration standards should involve a broader audience
- On page 11, the report states that FDCC provides a baseline level of security; however, during meetings with GAO, the Department's National Institute of Standards and Technology has expressed that we do not consider FDCC to be a baseline.

We look forward to further communications with GAO regarding its conclusions.

Sincerely,


Gary Logke

See comment 1.

The following are GAO's comments on the Department of Commerce's letter dated February 18, 2010.

GAO Comment

1. In its March 2007 directives,¹ OMB stated that an objective of FDCC was to provide a baseline level of security to agencies. We used OMB's characterization of FDCC for this report.

¹OMB Memorandum for Chief Information Officers, March 20, 2007; OMB, M-07-11 (Mar. 22, 2007).

Appendix VI: Comments from the Department of Defense



NETWORKS AND
INFORMATION
INTEGRATION

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-6000

Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) draft report, GAO-10-202, "INFORMATION SECURITY: Agencies Need to Implement Federal Desktop Core Configuration (FDCC) Requirements" dated January 20, 2010 (GAO Code 311014).

I share the GAO conclusion that the FDCC initiative was an innovative approach by OMB to standardize and thereby strengthen information security at federal agencies.

I appreciate the opportunity to provide the enclosed comments on the draft report. My staff and I are responsible for overseeing the implementation of the GAO report recommendations. My point of contact for questions regarding FDCC is Mr. John Hunter, (703) 602-9927.

Sincerely,

Gary D. Guissanie
Acting Deputy Assistant Secretary of Defense
(Cyber, Identity and Information Assurance)

Enclosure:
As stated



**GAO DRAFT REPORT DATED JANUARY 20, 2010
GAO-10-202 (GAO CODE 311014)**

**“INFORMATION SECURITY: AGENCIES NEED TO IMPLEMENT
FEDERAL DESKTOP CORE CONFIGURATION REQUIREMENTS”**

**DEPARTMENT OF DEFENSE COMMENTS
TO THE GAO RECOMMENDATIONS**

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense complete implementation of the agency’s Federal Desktop Core Configuration (FDCC) baseline, including establishing firm milestones for completion. (See pages 51-52/GAO Draft Report)

DoD RESPONSE: Concur. The Department of Defense has made significant progress in implementing the FDCC baseline, and the Assistant Secretary of Defense (Networks and Information Integration) will work with the Components to establish firm milestones for completion.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them. (See pages 51-52/GAO Draft Report)

DoD RESPONSE: Concur. The Assistant Secretary of Defense (Networks and Information Integration) will work closely with the OSD staff and Components to ensure new acquisitions include FDCC settings.

ADDITIONAL RECOMMENDATION FROM DEPARTMENT OF DEFENSE: Contract language should be included in the Federal Acquisition Regulation (FAR) “to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.” This would provide the appropriate coverage for a Federal-wide IT contract issue.

RATIONALE: FDCC is a Federal Government-wide mandate not a Defense-specific acquisition requirement.

Appendix VII: Comments from the General Services Administration



GSA Administrator

February 22, 2010

The Honorable Gene L. Dodaro
Acting Comptroller General of the United States
U.S. Government Accountability Office
Washington, DC 20548

Dear Mr. Dodaro:

The U.S. General Services Administration (GSA) appreciates the opportunity to review and comment on the draft report, "Information Security: Agencies Need to Implement Federal Desktop Core Configuration (FDCC) Requirements" (GAO-10-202). The U.S. Government Accountability Office (GAO) recommends that the GSA Administrator improve the agency's implementation of FDCC.

We agree with the findings and recommendation and will take appropriate action. GSA will complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion.

If you have any additional questions or concerns, please do not hesitate to contact me. Staff inquiries may be directed to Ms. Kathleen Turco, Chief Financial Officer. She can be reached at (202) 501-1721.

Sincerely,


Martha Johnson
Administrator

cc: Mr. Gregory C. Wilshusen,
Director, Information Technology Security Issues
GAO

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
Telephone: (202) 501-0800
Fax: (202) 219-1243
www.gsa.gov

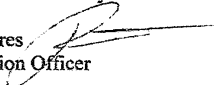
Appendix VIII: Comments from the Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528



**Homeland
Security**

MEMORANDUM FOR: Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office

FROM: Richard A. Spires 
Chief Information Officer

SUBJECT: Comment to GAO Report #10-202 "Information Security: Agencies
Need to Implement Federal Desktop Core Configuration
Requirements"

The Department of Homeland Security (DHS) Office of the Chief Information Officer (OCIO) has reviewed the findings of the Government Accountability Office (GAO) Report, #10-237 "Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements," dated February 2010.

The increase in security incidents and continuing weakness in security controls on information technology systems at federal agencies highlight the continuing need for improved information security. To standardize and strengthen agencies' security, the Office of Management and Budget (OMB), in collaboration with the National Institute of Standards and Technology (NIST), launched the Federal Desktop Core Configuration (FDCC) initiative in 2007. GAO was asked to (1) identify the goals, objectives, and requirements of the initiative; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiative; and (3) identify the benefits, challenges, and lessons learned in implementing this initiative. To accomplish this, GAO reviewed policies, plans, and other documents at the 24 major executive branch agencies; reviewed OMB and NIST guidance and documentation; and interviewed officials.

GAO recommended that DHS take four actions to improve the Department's implementation of FDCC. OCIO's comments on the specific recommendations are as follows:

Recommendation #1: Complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion.

OCIO March 2010 Response: OCIO concurs. DHS developed a FDCC draft baseline which is currently under review by the designated accrediting authority. A copy of the FDCC draft baseline and the FDCC compliance milestone tracking status is enclosed for your reference.

Recommendation #2: Develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority.

OCIO March 2010 Response: OCIO concurs. DHS has developed a process to approve deviations from the FDCC baseline, which is maintained and controlled by the DHS Infrastructure Change Control Board (ICCB). A copy of the draft "FDCC Baseline Update Process" is enclosed for your reference.

Recommendation #3: Develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.

OCIO March 2010 Response: OCIO concurs. Each DHS Component has chosen a NIST-validated SCAP tool that best fits into its IT infrastructure. Below is a list of the SCAP tools used by each Component to monitor their FDCC compliance:

- Customs and Border Protection uses Big Fix.
- U.S. Citizenship and Immigration Services uses McAfee.
- Federal Emergency Management Agency uses Tenable Nessus.
- Federal Law Enforcement Training Center uses Tenable Nessus and McAfee.
- DHS Headquarters uses Tenable Nessus and McAfee.
- Immigration and Customs Enforcement uses Big Fix.
- DHS Office of Inspector General uses Tenable Nessus.
- Transportation Services Administration uses Secure Elements C5.
- U.S. Coast Guard uses Secutor Prime.
- U.S. Secret Service uses Threat Guard.

Recommendation #4: Ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

OCIO March 2010 Response: OCIO concurs with caveat. DHS already has regulations in place to ensure new acquisitions meet FDCC requirements. The Department of Homeland Security Acquisition Regulation (HSAR) of June 2006 establishes uniform acquisition policies and procedures, which implement and supplement the Federal Acquisition Regulation (FAR).

HSAR Section 3052.204-70 "Security requirements for unclassified information technology resources of the HSAR" states:

Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when

accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

DHS Sensitive System Policy Publication 4300A, ID 3.7.e states:

“Workstations shall be configured in accordance with DHS guidance on FDCC.”

Enclosures:

- DHS FDCC baseline
- DHS FDCC compliance milestone tracking status
- DHS FDCC Baseline Update Process
- MD 4300A “DHS Sensitive Systems Policy Directive 4300A”
- 311014 DRAFT GAO #10-202 for Agency Comment, “Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements”

Appendix IX: Comments from the Department of Housing and Urban Development

Note: GAO's comments supplementing those in the report's text appear at the end of this appendix.



U.S. DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT
WASHINGTON, D.C. 20410-3000

OFFICE OF THE CHIEF INFORMATION OFFICER

FEB 17 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the Government Accountability Office (GAO) draft report entitled, Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements (GAO-10-202).

The Department of Housing and Urban Development reviewed the draft report and concurs with the following recommendations for Executive Actions:

- acquire and deploy a NIST-validated SCAP tool to monitor compliance with FDCC;
- develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool;

With respect to the above items, HUD anticipates a contract award in the 3rd quarter of Fiscal Year 2010, with implementation by September 30, 2010.

However, HUD provides the following comments to address the remaining recommendations:

- develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority;

The Department has developed a FDCC Waiver Request Standard Operating Procedure (SOP). In response to a GAO request, the attached document was provided on December 15, 2009.

- ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

See comment 1.

See comment 2.

**Appendix IX: Comments from the Department
of Housing and Urban Development**

2

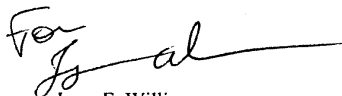
Attached is a standard contract clause that the HUD Chief Procurement Officer issued in June 2007 for use in all IT contracts. HUD is in compliance with the above language requirement for new acquisitions.

The Department remains committed to improving information security and reducing Information Technology operating costs, the major goals of the FDCC. More definitive information with timelines will be provided once the final report has been issued.

If you have any questions or require additional information, please contact Jerry E. Williams, Chief Information Officer, at 202-708-0306.

Enclosure

Sincerely,



Jerry E. Williams
Chief Information Officer

The following are GAO's comments on the Department of Housing and Urban Development's letter dated February 17, 2010.

GAO Comments

1. After reviewing additional documentation provided by department representatives, we agreed that the department had met the requirement and modified the column "have policy to approve deviations by designated authority" in table 4 from "no" to "yes." The recommendation to this finding was removed from the report.
2. After subsequent discussion with department representatives, they orally concurred with our recommendation.

Appendix X: Comments from the Department of the Interior



United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240



FEB 23 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for providing the Department of the Interior the opportunity to review and comment on the draft Government Accountability Office Report entitled, *"INFORMATION SECURITY: Agencies Need to Implement Federal Desktop Core Configuration Requirements"* (GAO-10-202).

The Department concurs with the recommendations subject to the modifications suggested in the enclosure.

We hope the technical comments and the additional information provided will assist you in preparing the final report. If you have any questions, or need additional information, please contact the Department's Chief Information Security Officer (CISO), Lawrence K. Ruffin, at (202) 208-5419 or Davene Barton at (202) 208-5438.

Sincerely,

A handwritten signature in black ink, appearing to read "Rhea Suh".

Rhea Suh
Assistant Secretary
Policy, Management and Budget

Enclosure

Appendix XI: Comments from the Department of Labor

Note: GAO's comments supplementing those in the report's text appear at the end of this appendix.

U.S. Department of Labor

Office of the Assistant Secretary
for Administration and Management
Washington, D.C. 20210



FEB 12 2010

Gregory C. Wilshusen
Director, Information Security Issues
Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen:

This letter is provided in response to the draft report GAO-10-202, *Agencies Need to Implement Federal Desktop Core Configuration Requirements*, dated February 2010. We take seriously our responsibility to ensure the protection of our computer systems and information with which we are entrusted.

Overall, the draft reports provide a fair depiction of the Department of Labor (DOL) efforts to meet the OMB's mandate for implementing the Federal Desktop Core Configuration (FDCC). However I ask that the GAO reconsider their assessment regarding the Department's implementation of a National Institute of Standards and Technology (NIST)-validated Security Content Automation Protocol (SCAP) tool and FDCC acquisition language. The areas in the draft report to reconsider include:

- Page 26, Table 5: Through the deployment and use of ThreatGuard DOL has met the requirements for acquiring and utilizing a NIST-validated SCAP tool, thus the table should indicate a "Yes" response. DOL currently utilizes the tool to monitor all DOL agency FDCC baseline configurations and also conducts periodic scans of agency baselines configuration to ensure continuing compliance.
- Page 28, Table 6: All appropriate new contracts awarded since the issuance of the OMB mandate includes the required FDCC acquisition language as appropriate, thus the table should indicate partial implementation. This statement is further supported by the FY09 OIG FISMA assessment results. DOL acknowledges that challenges exist in updating legacy contracts issued prior to OMB mandate. Additionally, DOL has begun a comprehensive exercise to review and modify all appropriate legacy contracts to include the required FDCC language over the next 18 months.
- Page 55, Bullet 1: Recommends DOL complete deployment of a NIST-validated SCAP tool to monitor FDCC compliance. DOL has implemented a NIST-validated SCAP tool called ThreatGuard. The tool provides DOL adequate capabilities for monitoring its compliance with FDCC and other NIST issued SCAP content. DOL is planning to enhance its use of ThreatGuard and other DOL implemented NIST-validated SCAP tools to provide real-time monitoring of baseline configurations in Fiscal Year 2011.
- Page 55, Bullet 2: Recommends DOL ensure FDCC language is included in contracts. As mentioned above, all new contacts comply with the FDCC mandate. DOL plans to modify all legacy contracts to included the required FDCC language over the next 18 months.

See comment 1.

See comment 2.


See comment 3.

See comment 4.

**Appendix XI: Comments from the Department
of Labor**

Thank you again for the opportunity to comment on the draft report. If you have any questions or you require further discussion about our comments, please have your staff contact Mrs. Tonya Manning, DOL Chief Information Security Officer, at Manning.Tonya@dol.gov or 202-693-4431.

Sincerely,



T. Michael Kerr

Assistant Secretary for Administration and Management
Chief Information Officer

The following are GAO's comments on the Department of Labor's letter dated February 12, 2010.

GAO Comments

1. After reviewing additional documentation provided, we agreed that the department had met the requirement and modified the column "NIST-validated SCAP tool acquired and deployed" in table 5 from "no" to "yes."
2. After reviewing additional documentation provided by department representatives, we agreed that the department had partially met the requirement and modified the column "language incorporated" in table 6 from "no" to "partially."
3. The recommendation to this finding was removed (see comment 1).
4. The recommendation to this finding was modified as appropriate (see comment 2).

Appendix XII: Comments from the National Aeronautics and Space Administration

National Aeronautics and Space Administration
Headquarters
Washington, DC 20546-0001



FEB 19 2010

Reply to Attn of: Office of the Chief Information Officer

Mr. Gregory C. Wilshusen
Director, Information Security Issues
United States Government Accountability Office
Washington, DC 20548

Dear Mr. Wilshusen:

The National Aeronautics and Space Administration (NASA) appreciates the opportunity to review and comment on the draft report entitled, "Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements" (GAO-10-202).

In the draft report, GAO makes one recommendation relating to NASA's implementation of Federal Desktop Core Configuration (FDCC) requirements, specifically:

Recommendation: To improve the agency's implementation of FDCC, we recommend that the Administrator of the National Aeronautics and Space Administration complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion.

Response:

NASA will establish firm milestones to complete an implementation of the agency's FDCC baseline while exercising caution not to disable unique mission orientated capabilities. IT security is a compromise between available capabilities and applicable controls.

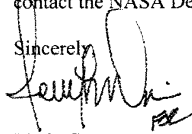
NASA set a goal for 85 percent of the agency systems within the defined FDCC software and system scope to comply with the original core configuration requirement. NASA believes general purpose office automation systems are more amenable to the use of the FDCC controls than systems which provide Agency mission-unique functions. Therefore, the 85 percent implementation baseline goal represents an operational reality and offers a reasonable balance between security configuration and operational necessities.

NASA would like to note that future guidance and configurations must keep pace with industry updates in common operating systems and applications. The FDCC technical guidance and policy releases tend to lag behind software releases. In order to remain relevant and viable, FDCC technical and policy development must advance at the pace of Federal Agency procurements of new commercial software.

**Appendix XII: Comments from the National
Aeronautics and Space Administration**

Thank you for the opportunity to review the draft report. We look forward to your final report to Congress. If you have any questions or require additional information, please don't hesitate to contact the NASA Deputy CIO for IT Security, Jerry Davis at (202) 358-1401.

Sincerely,



Linda Cureton
Chief Information Officer

Appendix XIII: Comments from the Office of Personnel Management

Note: GAO's comments supplementing those in the report's text appear at the end of this appendix.



Office of the Director

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

MEMORANDUM FOR GREGORY C. WILSHUSEN
DIRECTOR
GOVERNMENT ACCOUNTABILITY OFFICE

FROM: MATTHEW E. PERRY
CHIEF INFORMATION OFFICER *Matthew E. Perry*
03/02/2010

Subject: Government Accountability Office Audit Regarding Agencies
Need to Implement Federal Desktop Core Configuration
Requirements

This memorandum is in response to the GAO (Government Accountability Office) audit finding released in February of 2010, GAO-10-202 Federal Desktop Core Configuration (FDCC). This memorandum will address two areas; comments specific to the factual representations within the report, as well as a response to the recommendations section of the report.

Comments specific to the report:

1. Page 24, Table 4 states that the Office of Personnel Management (OPM) did not provide deviations and had no policy to review deviations. This is incorrect. OPM provided Office of Management and Budget (OMB) the list of deviations for their data call on March 31 2008. OPM has updated its workstation configuration policy to require that deviations be documented and approved through our Change Control process. Both of these artifacts were provided to GAO during their engagement.
2. Page 43-44, "GAO recommends that OMB, among other things, issue explicit guidance on assessing the risks of deviations and monitoring compliance with FDCC. GAO also recommends that agencies take steps to fully implement FDCC requirements." For FDCC to be successful, the guidance should come with funding.
3. Page 3, The initiative mandated that Federal agencies implement standardized configuration settings on workstations with Windows XP or Vista operating systems. FDCC needs to be updated to include Windows7.

Response to the GAO Audit Recommendations:

Finding: "complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion;"

Response: OPM has completed several significant milestones for OPM's FDCC compliance including integrating FDCC compliance into the new image creation process for PCs deployed after March 2008. This ensures that all new PCs adhere to OPM

See comment 1.

standards for FDCC compliance. OPM has not established a timeline for testing and evaluating images that were deployed prior to the FDCC adoption in March of 2008. OPM has a FY 2010 project defined to coordinate the testing of FDCC settings with OPM legacy images and test all legacy COTS and custom developed applications for interoperability. Due to the complexity of this initiative, we anticipate that this project will be completed in 2011.

Finding: "document deviations to FDCC and have them approved by a designated accrediting authority;"

Response: OPM has been documenting deviations for all FDCC settings since 2008. All images along with the deviations presently go through the OPM Change Control Board (CCB) for approval and documentation. This CCB process is in line with the accreditation boundary of the LAN/WAN general support system which includes image security controls and is monitored as part of OPM's continuous monitoring processes.

See comment 2,

Finding: "develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority;"

Response: OPM has updated and provided GAO the OPM Workstation Hardening Policy which details the FDCC requirements as well as the requirements to monitor and manage deviations within our change control processes.

Finding: "ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them."

Response: In practice, the FDCC language has been inserted into major IT initiatives ongoing at OPM, however, standard language has not been universally adopted within all contracts. The CIO's office will work to make the language standard in all new contracts and identify the best means to address contract modifications for existing contracts.

In summary, OPM has addressed many of the FDCC compliance requirements and all laptop computers and images deployed after March 2008 adhere to the FDCC security settings. Additional projects are underway to address legacy images to ensure uniform compliance.

The following are GAO's comments on the Office of Personnel Management's letter dated March 2, 2010.

GAO Comments

1. After subsequent discussion with agency representatives, they orally concurred with our recommendation.
2. After reviewing additional documentation provided by agency representatives, we agreed that the agency had met the requirement and modified the column "have policy to approve deviations by designated authority" in table 4 from "no" to "yes." The recommendation to this finding was removed from the report.

Appendix XIV: Comments from the Social Security Administration



SOCIAL SECURITY

The Commissioner

March 2, 2010

Mr. Gregory Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to review and comment on the Government Accountability Office (GAO) draft report, "INFORMATION SECURITY: Agencies Need to Implement Federal Desktop Core Configuration Requirements" (GAO-10-202). Attached is our response to the report.

If you have any questions, please contact me or have your staff contact Candace Skurnik, Director, Audit Management and Liaison Staff at (410) 965-4636.

Sincerely,

Michael J. Astrue

Enclosure

SOCIAL SECURITY ADMINISTRATION BALTIMORE, MD 21235-0001

COMMENTS ON THE GOVERNMENT ACCOUNTABILITY OFFICE (GAO) DRAFT REPORT, "INFORMATION SECURITY: AGENCIES NEED TO IMPLEMENT FEDERAL DESKTOP CORE CONFIGURATION (FDCC) REQUIREMENTS" (GAO-10-202)

Recommendation 1

Develop, document, and implement a policy to approve deviations to FDCC by a designated accrediting authority.

Comment

We agree. We already have a formal systems security policy that we used to approve deviations to FDCC. Our policy and process for managing security configurations is contained in our Information Systems Security Handbook, Chapter 17. We will review this policy to ensure that it adequately documents the review and approval of FDCC deviations.

As an agency that manages more than 100,000 Windows systems, we take the implementation of the FDCC settings very seriously. We continually look for ways to reduce our exposure to cybersecurity threats and protect our network and systems. Since the announcement of Commonly Accepted Security Configurations for Windows Operating Systems in 2007, we have successfully met all FDCC milestones. We have procured a validated Security Content Automation Protocol (SCAP) product, tested our Windows configuration settings using the SCAP product, and provided justification for SCAP deviations. Many of the SCAP deviations we found are the result of more stringent agency settings that exceed the FDCC standard. Our Office of Systems maintains approved security configurations for Windows-based systems that incorporate FDCC settings to securely accomplish our mission. We conduct regular security assessments to review our approved security configurations.

Recommendation 2

Complete deployment of a NIST-validated SCAP tool to monitor compliance with FDCC.

Comment

We agree. We are currently testing McAfee's National Institute of Standards and Technology (NIST)-validated Security Content Automation Protocol (SCAP) tool and anticipate deployment by the end of April 2010.

Recommendation 3

Develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool.

Comment

We agree. We will finalize our policy to monitor FDCC compliance as we approach completion of NIST-validated SCAP tool testing.

Recommendation 4

Ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

Comment

We agree. We will include language in our contracts to ensure that new acquisitions include FDCC settings and that information technology products can operate effectively using the settings, where appropriate.

Appendix XV: Comments from the Department of the Treasury



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

FEB 12 2010

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
410 G Street, NW
Washington, DC 20548

Thank you for your draft report on "*Information Security: Agencies Need to Implement Federal Desktop Core Configuration Requirements.*" In demonstrating our commitment to the Federal Desktop Core Configuration (FDCC) initiative, Treasury has implemented the 674 FDCC settings on the Department's 130,000 personal computers and laptops.

The Department appreciates GAO's recommendations to complete the implementation of our FDCC baseline and to incorporate contract language to ensure new acquisitions include FDCC settings and products of IT providers operate effectively when using them. Responding to these recommendations, the Department has developed language for new acquisition contracts and anticipates completing implementation in Fiscal Year 2010 for one remaining bureau. Additionally, the Department has now completed implementation of its baseline with 100% of its personal computers and laptops being FDCC compliant. With these accomplishments, Treasury will receive the maximum protection and benefit from FDCC guidelines.

Thank you for your important efforts during this review. Please do not hesitate to contact me at 202-622-1200 should you have any questions.

Sincerely,

A handwritten signature in black ink, appearing to read "Michael D. Duffy".

Michael D. Duffy
Deputy Assistant Secretary for Information Systems
and Chief Information Officer

Appendix XVI: Comments from the U.S. Agency for International Development



USAID
FROM THE AMERICAN PEOPLE

FEB 18 2010

Mr. Thomas Melito
Director
International Affairs and Trade
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Melito:

I am pleased to provide the U.S. Agency for International Development's (USAID) formal response on the draft GAO report entitled, "Information Security Agencies Need to Implement Federal Desktop Core Configuration Requirements" (GAO-10-202).

The enclosed USAID comments are provided for incorporation with this letter as an appendix to the final report.

Thank you for the opportunity to respond to the GAO draft report and for the courtesies extended by your staff in the conduct of this audit review.

Sincerely,

A handwritten signature in black ink that reads "Drew W. Luten".

Drew W. Luten
Senior Deputy Assistant Administrator
Bureau of Management

Enclosure: a/s

U.S. Agency for International Development
1300 Pennsylvania Avenue, NW
Washington, DC 20523
www.usaid.gov

USAID COMMENTS ON GAO DRAFT REPORT No. (GAO-10-202)

GAO Recommendation 1: To improve the agency's implementation of FDCC, we recommend that the Administrator of the Agency for International Development take the following action:

- Ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

USAID Management Response: USAID concurs with the recommendation.

Appendix XVII: Comments from the Department of Veterans Affairs



Department of Veterans Affairs
Office of the Secretary

March 8, 2010

Mr. Gregory C. Wilshusen
Director
Information Security Issues
441 G Street, NW
Washington, DC 20548

Dear Mr. Wilshusen:

The Department of Veterans Affairs (VA) has reviewed the Government Accountability Office's (GAO) draft report, **INFORMATION SECURITY: Agencies Need to Implement Federal Desktop Core Configuration Requirements** (GAO-10-202). VA agrees with GAO's conclusions and concurs with GAO's four recommendations to the Department.

The enclosure provides specific details on VA's actions to GAO's recommendations. VA appreciates the opportunity to comment on your draft report.

Sincerely,


John R. Gingrich
Chief of Staff

Enclosure

Enclosure

Department of Veterans Affairs (VA) Comment to
Government Accountability Office (GAO Draft Report
***INFORMATION SECURITY: Agencies Need to Implement Federal
Desktop Core Configuration Requirements***
(GAO-10-202)

GAO recommendation: To improve the department's implementation of FDCC, we recommend that the Secretary of Veterans Affairs take the following four actions:

Recommendation 1: Complete implementation of the agency's FDCC baseline, including establishing firm milestones for completion.

VA Comments: Concur. The target date for completion of all FDCC baseline settings is September 30, 2010. A project plan, complete with milestones, has been established to monitor FDCC compliance.

GAO Recommendation 2: Acquire and deploy a NIST-validated SCAP tool to monitor compliance with FDCC.

VA Comments: Concur. The VA owns three SCAP tools; however, due to challenges involved in deploying each, none have been implemented to date. VA plans to overcome these challenges and complete implementation by September 30, 2010.

GAO Recommendation 3: Develop, document, and implement a policy to monitor FDCC compliance using a NIST-validated SCAP tool.

VA Comments: Concur. A project plan has been established to monitor FDCC compliance. The target date for issuance of a draft policy and handbook (procedures) is September 2010.

GAO Recommendation 4: Ensure that language is included in contracts to ensure new acquisitions include FDCC settings and products of information technology providers operate effectively using them.

VA Comments: Concur. Draft VA Handbook 6500.6, *Contract Security* (currently in final review by VA Records Management) provides the following language that can be added to contracts, as appropriate, regarding FDCC. The highlighted revisions address future versions of browsers and operating systems.

Enclosure

Department of Veterans Affairs (VA) Comment to
Government Accountability Office (GAO Draft Report
**INFORMATION SECURITY: Agencies Need to Implement Federal
Desktop Core Configuration Requirements**
(GAO-10-202)

INFORMATION SYSTEM DESIGN AND DEVELOPMENT

Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference Appendix D of VA Handbook 6500, VA Information Security Program). During the development cycle a Privacy Impact Assessment (PIA) must be completed, provided to the COTR, and approved by the VA Privacy Service in accordance with Directive 6507, VA Privacy Impact Assessment.

The contractor/subcontractor shall certify to the COTR that applications are fully functional and operate correctly as intended on systems using the VA Federal Desktop Core Configuration (FDCC) once approved, and the common security configuration guidelines provided by NIST or the VA. This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista).

The standard installation, operation, maintenance, updating, and patching of software shall not alter the configuration settings from the VA approved and FDCC configuration. Information technology staff must also use the Windows Installer Service for installation to the default "program files" directory and silently install and uninstall.

Appendix XVIII: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory C. Wilshusen, (202) 512-6244 or wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individual named above, Jeffrey Knott (Assistant Director), John Bainbridge, William Cook, Kami Corbett, Neil Doherty, Michele Fejfar, Nancy Glover, Valerie Hopkins, Lee McCracken, Zsarog Powe, Carl Ramirez, and Shawn Ward made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, <http://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

