AUDIT OF NARA'S IMPLEMENTATION OF THE FEDERAL DESKTOP CORE CONFIGURATION

OIG Report No. 08-10

August 26, 2008

EXECUTIVE SUMMARY

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of NARA's implementation of the Federal Desktop Core Configuration (FDCC). During the audit, we evaluated NARA's status of implementing FDCC; plans for applying FDCC across the enterprise; and reports to the Office of Management and Budget (OMB) to determine whether NARA had adequately implemented FDCC as required by OMB.

FDCC is an OMB mandated security configuration checklist[1] for Microsoft Windows XP and Vista Operating system software. Developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DOD), and the Department of Homeland Security (DHS), FDCC is a set of operating-system configurations, such as password requirements and turning off unused services, designed to ensure security. In March 2007, OMB directed agencies using Windows XP and Vista to adopt these security configurations. Agencies were required to submit their draft implementation plans to OMB by May 1, 2007 and adopt the standard security configurations by February 1, 2008.

Our review found that NARA missed the deadline for implementation of the OMB mandated FDCC settings and inaccurately reported their status to OMB. Additionally, NARA has not:

(a) Developed sufficient implementation and test plans;
(b) Developed plans to resolve identified deviations from FDCC; and
(c) Enforced FDCC password settings.

The use of a standardized security configuration checklist, such as FDCC, can reduce the vulnerability exposure of IT products and be particularly helpful to small organizations for securing their systems. The FDCC settings were developed to improve information security and overall network performance while lowering operating costs. Effective and well-tested security configurations mean less time and money is spent eradicating malware[2], restoring systems from backups, and reinstalling operating systems and applications. By not implementing these configurations, NARA is not able to achieve these benefits and mitigate their cyber security risks.

We made five recommendations that when implemented will assist NARA in implementing the mandated FDCC configurations.

[1] A security configuration checklist is a series of documented instructions for configuring a product to a pre-defined operational environment.

[2] Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malware includes computer viruses, worms, Trojan horses, spyware, and other malicious and unwanted software.

BACKGROUND

On March 22, 2007, OMB issued memorandum, M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, directing agencies who use Windows XP and Vista to adopt the security configurations developed by NIST, DoD, and DHS. While not addressed specifically as "Federal Desktop Core Configuration", the FDCC was originally called for in this memo to all Federal agencies and department heads and in a corresponding memorandum, *Establishment of Windows XP and VISTA Virtual Machine Procedures for Adopting the Federal Desktop Core Configurations*, from OMB to all Federal agency and department Chief Information Officers (CIOs). Agencies with these operating systems were required to submit their draft implementation plans to OMB by May 1, 2007 and adopt the standard security configurations by February 1, 2008. NARA employs the Windows XP operating system and thus falls within this population.

To develop the FDCC settings, DoD worked with NIST and DHS to reach a consensus agreement on security configurations for Windows XP desktops. The Windows XP FDCC is based on the Air Force's customization of the recommendations in NIST Special Publication (SP) 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, which was created in October 2005 to assist IT professionals in effectively securing Windows XP Professional Systems. With these settings, information is more secure, overall network performance is improved, and overall operating costs are lowered.

In order to report compliance with FDCC, NIST developed a suite of interoperable and automatable security standards know as the Security Content Automation Protocol (SCAP). To achieve the goals set forth in OMB Memorandum M-07-11, it is necessary for agencies to have a security configuration scanning tool that uses official SCAP content. Through the use of SCAP compliant tools and official FDCC SCAP content, agencies can routinely monitor their system to ensure that the FDCC settings have not been altered as a result of patching, installation of new software, or human interaction. The tools compare the deployed configuration against the official SCAP FDCC content and report on any discrepancies so corrective action can be taken.

As an integral part of the continuous monitoring of systems configured to FDCC, agencies must report their testing results to OMB and NIST. Using the SCAP reporting format enables NIST to effectively collect and organize the results for analysis and trending over time. NIST will aggregate the results from all agencies, but will not generally provide direct feedback to each individual agency concerning their results.

NARA's Office of Information Services (NH) manages all matters relating to information technology programs, projects, processes, and infrastructure. NH is responsible for ensuring that NARA's IT program conforms to all NARA and Federal standards, policies, and guidelines for interconnectivity and interoperability, computer system efficiency, and computer security. Within NH, the Information Technology Services Division (NHT) oversees the delivery of network and computer services across the enterprise and the Information Technology Security Staff (NHI) develops and maintains

NARA's agency-wide information technology security program. Members of NHT and NHI are working together to implement the FDCC settings at NARA.

NARA has about 4,100 Windows XP workstations located at Archives I, Archives II, and various regional offices around the country. Currently, there are 12 variants of a Windows XP Professional baseline image running on these workstations. NARA plans to create and deploy a new baseline image complaint with the FDCC settings by July 28, 2008. With the use of Novell ZENworks[3], NARA plans to automatically distribute and manage the FDCC settings for their Windows XP workstations. To report their compliance to OMB, NARA purchased ThreatGuard's Secutor Prime software, which is capable of using NIST's SCAP content.

OJECTIVE, SCOPE, METHODOLOGY

The objective of this audit was to determine whether NARA had adequately implemented the FDCC settings as required by OMB. Specifically, we determined whether NARA (a) met the OMB mandated deadline; (b) adequately reported their status to OMB; and (c) developed adequate plans for implementing FDCC across the enterprise.

We examined applicable laws, regulations, NARA guidance, and other IT-related guidance, including (a) Federal Information Security Management Act; (b) OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*; (c) NIST SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*; (d) NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklist Users and Developers*; and (e) NARA Interim Guidance 804-2, *NARANET Password Requirements*.

To accomplish our objective, we reviewed and analyzed: (a) NARA's FDCC status reports and implementation plans submitted to OMB; (b) deviation reports; (c) Request for Change (RFC) for the deployment of current standard Group Policy/Windows Operating System Settings; and (d) Plan of Action and Milestones (POA&Ms). In addition, we interviewed the NARA CIO and NH officials responsible for implementing FDCC to determine whether they were able to meet the OMB mandated deadline and identify any possible constraints in the meeting the deadline.

Our audit work was performed at Archives II in College Park, MD between April 2008 and July 2008. We conducted this performance audit 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.

[3] Novell ZENworks uses a Policy-Driven Automation to reduce and in some cases eliminate desktop management tasks such as software distribution, software repair, desktop configuration, workstation imaging, remote management, and workstation inventory throughout the lifecycle of the device.

FINDINGS AND RECOMMENDATIONS

FDCC Settings Not Implemented

NARA missed the deadline for implementing the OMB mandated FDCC settings across their enterprise. This condition occurred because of lack of management attention, resources, and experience with automated tools. OMB Memorandum M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, required agencies to adopt the standard security configurations (FDCC) by February 1, 2008. According to an OMB official, OMB expects agencies to implement the requirements of memoranda on a timely basis. By not implementing these settings, NARA desktops are not set to the most secure and restricted configuration settings.

In their February 6, 2008 submission to OMB, NARA reported that none of its 4,100[4] Windows XP desktops were fully compliant with the FDCC. According to an NH official, NARA has no method or tool in place to determine the level of compliance for the workstations currently used. However, scans conducted by an NH official in December 2007 and April 2008 of two existing workstations reported that they were 57% and 67% compliant with FDCC. In March 2008, NARA developed a standard baseline image[5] for desktops that was reported by NH as 92% compliant with the FDCC settings. However, this image is not scheduled to be deployed to NARA desktops until July 28, 2008, almost six months past the OMB deadline.

NARA was not able to implement FDCC due to a lack of management attention, resources, and experience with automated tools. The FDCC Request for Change (RFC)[6] was not submitted for approval until March 13, 2008, almost six weeks after the OMB set deadline. In addition, NH officials were not assigned responsibility for implementing FDCC until after the OMB deadline. We were informed by the CIO that resources were not available for the implementation of FDCC prior to the deadline; however, additional resources were not identified or requested during this time. According to the CIO, NH did not have the funding, manpower, or tools to implement FDCC. Further, NARA did not have a plan or prior experience using Novell ZENworks to distribute or to manage Windows XP desktop settings.

Consequently, NARA desktops are not set to the most secure and restricted configuration settings. The FDCC settings were developed to improve information security and overall network performance while lowering operating costs. By not implementing these

[4] In the submission to OMB, NARA incorrectly reported 4,400 workstations. The number of workstations reported should have been 4,100.

[5] A standard baseline image is a set of standard software, which usually includes the operating system (e.g. Windows XP), word processing, spreadsheet, presentation, and database management software (e.g. Office XP), along with an Internet browser (e.g., MS Internet Explorer or Netscape) and an e-mail package (e.g. GroupWise), that is preloaded on each desktop.

[6] RFCs are forms used to submit, track, and manage requests for changes to configuration items that comprise the NARA Enterprise Architecture (EA) work products when those changes are not identified as part of the EA Program Plan.

configurations, NARA is not able to achieve these benefits and mitigate their cyber security risks.

Recommendation 1

The CIO should:

(a) Define those resources required to implement FDCC and seek additional funding if required.

(b) Develop a plan to automate the distribution of FDCC settings to individual desktops.

Management Comment(s)

Management concurred with recommendations and indicated that actions have been completed.

OIG Response to Management Response

We disagree with part of management's position. While we did receive the latest Request for Proposal (RFC), which included an approach to implement the FDCC settings, the finding remains open. NARA has not completed the implementation of the FDCC. As of August 19, 2008, FDCC settings have been successfully applied to about 76 percent of NARA's desktops (3,123 of approximately 4,100). In addition, failures were identified in at least 298 desktops and remain unresolved.

Inaccurate Reporting to OMB

The status report submitted to OMB on March 31, 2008 was inaccurate and did not meet OMB's reporting guidelines to demonstrate compliance with OMB M-07-11. This condition occurred because NARA had no automated method or tool in place to determine the level of compliance for the workstations currently in use. By not accurately reporting to OMB, OMB is not aware of NARA's current status and NIST cannot make any necessary changes to the FDCC program.

OMB Memorandum M-07-11 required agencies to adopt the standard security configurations (FDCC) and subsequent NIST and OMB instructions required agencies to report the details of their implementation status. Specifically, OMB and NIST required agencies to report computer counts and FDCC deviations[7] for each operational environment/system present within the agency. Agencies were required to report on a single representative computer for each combination of environment/system role and FDCC operating system and then report the number of FDCC deviations.

[7] For each FDCC setting, NIST assigned an identification number. Agencies were required to submit the total number of non-compliant FDCC settings and list them by their identification number.

In their March 31, 2008 report to OMB, NARA reported on a sample of three desktops that contained the new baseline image, which had not been deployed enterprise wide. Therefore, the sample was not representative of NARA's currently Centrally Managed General Purpose Desktop Environment and the number of deviations was not representative of NARA's implementation status. While NARA reported only 18 FDCC deviations, the deployed desktops used by the agency had numerous deviations. Specifically, a scan of an existing desktop showed at least 119 deviations from the FDCC settings.

In addition, NARA did not report on all of the operational environments/systems within the agency. Subsequent to the submission, a NH official identified additional desktops that were not captured in their March 2008 report to OMB. These additional desktops are part of NARA's classified systems, which use the Windows XP operating system, but are not part of the Centrally Managed General Purpose Desktop Environment.

NARA was unable to report on the compliance of their workstations currently in use because of the variety of baselines installed on these workstations. Currently, there are 12 variants of a Windows XP Professional baseline image running on these workstations. These settings are not currently managed through a central method, which restricts the ability to verify the level of compliance of all enterprise workstations. NH officials decided not to expend resources in testing the compliance of each of these baselines and any variants. Instead, they reported on the baseline that was created to be in compliance with FDCC. Additionally, the OMB submission did not allow for additional comments for NH officials to provide clarifying statements.

By not accurately reporting to OMB, OMB is not aware of NARA's current status and NIST cannot make any necessary changes to the FDCC program. In addition, NARA has no basis for requesting additional resources to implement FDCC settings.

Recommendation 2

We recommend the CIO provide a disclaimer statement in their next status report to OMB, stating that the sample is not representative of their current environment and an explanation.

Management Comment(s)

Management concurred with recommendation.

Implementation and Test Plans Not Developed

NARA did not develop sufficient implementation and test plans for applying FDCC settings across the enterprise as required by OMB and recommended by NIST. This condition occurred because of a lack of staffing resources and management attention. Without adequate plans, NARA's successful implementation of FDCC could be at risk.

Implementation Plans

OMB Memorandum, M-07-11, required agencies to develop draft implementation plans for Commonly Accepted Security Configurations (FDCC) and submit the plans to OMB by May 1, 2007. A subsequent OMB Memorandum to agency CIO's outlined the required elements for the implementation plans. According to this memo, implementation plans should have described various items such as testing, implementing, and automating enforcement of these configurations.

In the implementation plan submitted to OMB on April 30, 2007, NARA briefly addressed each of the required items. However, none of the items addressed how NARA would implement the FDCC for their Windows XP desktops. For example, NARA's response to "ensuring these configurations are incorporated into agency capital planning and investment control (CPIC) processes" only stated the following:

> An integral component of NARA's CPIC process is a review of potential investments by the agency Enterprise Architecture Review Board (ARB). The ARB was constituted in December 2006. Conformance to the agency approved Technology Standards Profile is considered to be part of the technical review process within the ARB.

NARA's response did not indicate whether implementing these configurations was incorporated in their CPIC process. We found that the FDCC requirement had not been included in NARA's CPIC process, which ensures that senior management has the timely, accurate information required to authorize information systems development and financial commitments. If the FDCC requirement was included in NARA's CPIC process, adequate plans and resources could have been developed and assigned. Therefore, the plans submitted to OMB were not sufficient to implement FDCC settings.

In March 2008, a month after the OMB deadline, the Information Technology Services Division (NHT) recommended two approaches to bring all workstations into compliance with FDCC. The first was through the use of the PC Refresh[8] and the second was through the development of centrally managed security policies that could be deployed to current workstations. However, as of May 2008, formal plans and schedules to implement these two approaches have not been developed.

[8] During the PC Refresh, NHT will replace 25% of the current workstations within NARANet. All of the new workstations will receive the 92% FDCC compliant baseline image.

Test Plans

According to NIST, adequate testing is an important element in implementing new security settings, such as FDCC. Prior to introducing any system modification in the production environment, configurations should be tested in a non-production environment[9] to identify adverse effects on system functionality. NIST recommends testing for all security controls to determine what impact they have on system security, functionality, and usability, and taking appropriate steps to address any significant issues. With regards to FDCC settings, NIST stated that there are a number of settings which will impact system functionality and agencies should test thoroughly before they are deployed in an operational environment.

We found that Test Plans have not been developed for testing the FDCC settings at NARA. One contractor involved in the process warned that there will have to be some extensive testing with the following NARA systems: Order Fulfillment and Accounting System (OFAS), Records Management Application (RMA), and Case Management and Reporting System (CMRS). Despite this warning, test plans have not been developed.

Implementation and test plans were not developed due to a lack of staffing resources and lack of management attention. When asked why resources were not allocated to develop plans for implementing FDCC, the CIO stated, "It is difficult to keep up with all the OMB data calls and new requirements." Also, we were informed by NH officials that NARA had limited staff to test configurations and correct any identified problems. However, additional resources have not been identified or requested.

The OMB policy analyst heading the FDCC initiative was quoted as saying OMB "wants agencies to understand their universe and have a plan to get to FDCC compliance". Without adequate plans, the implementation of FDCC may not be successful. If adequate test plans are not developed, functionality or usability problems may not be identified and certain settings could cause unexpected problems.

After completion of our audit fieldwork, we were provided with test procedures for the installation of the FDCC settings on NARA workstations. We will analyze these procedures and provide our opinion in a subsequent reporting document.

Recommendation 3

We recommend the CIO to allocate resources to develop adequate implementation and testing plans.

Management Comment(s)

Management concurred with recommendation and indicated that actions have been completed.

[9] Non-production environments allow developers to test new configurations prior to implementing in the production environment.

OIG Response to Management Response

We disagree with part of management's position. While we did receive copies of the implementation and test plans, NARA has not successfully implemented the FDCC settings. In addition, our review of the test plans and results disclosed that the test results were incomplete and did not indicate how or if testing errors were corrected.

Plan of Action and Milestones Not Created

NARA has not developed adequate plans to resolve the identified deviations from FDCC as required by the Federal Information Security Management Act (FISMA) and OMB. This condition occurred because NH officials failed to include the FDCC deviations on their Plan of Action and Milestones (POA&M) and had no definitive plans for implementing most of the FDCC deviations. A similar finding was identified in OIG Report No. 08-05, *Audit of NARA's Compliance with the Federal Information Security Management Act for FY 2007*. By not including these deviations in a POA&M, the CIO may not have proper visibility of the deviations and cannot use the POA&M as an effective management tool to request and allocate resources to implement FDCC security settings.

FISMA requires Federal agencies to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies information security policies, procedures, and practices of the agency. OMB Memoranda M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, and M-04-25, *Reporting Instructions for the Federal Information Security Management Act*, provide instructions on how to implement a Plan of Action and Milestones (POA&M) process and information needed to report and track weaknesses identified. The purpose of the POA&M is to help agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

We found that NARA had not developed adequate plans to resolve the identified deviations from FDCC. Of the 18 deviations identified in NARA's proposed baseline image for Windows XP desktops, only four were included in a POA&M. The 14 deviations not included in a POA&M consist of settings related to passwords, encryption, automatic logons, and administrator account status.

Most of the 14 deviations were not included in a POA&M because NARA did not have definitive plans for implementing these items by a specified date. However, NH officials are now considering creating a single POA&M item to review the remaining FDCC setting deviations on a defined, periodic basis to evaluate what can be done to bring them in compliance.

By not including these deviations in a POA&M, the CIO may not have proper visibility of the deviations and cannot use the POA&M as an effective management tool to request and allocate resources to implement FDCC security settings.

Recommendation 4

We recommend the CIO include the remaining FDCC deviations in a POA&M and address each of these items.

Management Comment(s)

Management concurred with recommendation.

<u>Strong Password Requirements Not Implemented</u>

NARA has not implemented the required FDCC password settings. This condition occurred because NARA's password policy has not been updated for the use of strong passwords requirements. Additionally, weaknesses related to passwords, password management, and access controls have been identified in several past OIG Reports[10]. Without strong password requirements, NARA is at risk of an individual gaining unauthorized access, which can lead to the loss of data confidentiality and integrity.

FDCC follows the Password Policy Settings outlined in NIST SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, October 2005. These settings include enforcing password history, maximum password age, minimum password age, minimum password length, and complexity requirements. NARA's password requirements are outlined in NARA Interim Guidance 804-2, *NARANET Password Requirements*, dated December 11, 2001. This guidance describes the minimum length and complexity requirements for NARANET passwords.

Redacted pursuant to FOIA Exemptions b(2) and b(5)

Redacted pursuant to FOIA Exemptions b(2) and b(5)

[10] These reports include Audit of the NARA Systems Security Program, OIG Report No. 01-05; Firewall and Network Configuration Advisory Report, OIG Report No. 02-12; Evaluation of the NARA's Password Controls, OIG Report No. 04-23; and Audit of NARA's Network Perimeter, OIG Report No. 06-01.

[redacted]

When asked about constraints in implementing these settings, NH officials stated that one of these settings cannot be implemented because of a technical problem with Novell. ------Redacted pursuant to FOIA Exemption b(2)---- NH Officials were not aware of any other technical difficulties with the remaining password settings. However, NH officials perceive the settings will cause difficulties for desktop users. ----------------Redacted pursuant to FOIA Exemption b(2)---------------------------------- Perceived difficulties with conforming to FDCC settings do not validate nonconformance with government-wide requirements.

Access controls such as strong password requirements increase network and application security. Passwords are NARA's first line of defense in protecting user email accounts and other NARA information assets. Without strong password requirements, NARA is at risk of an individual, who is not permitted to access a system, to gain unauthorized access, which can lead to the loss of data confidentiality and integrity.

Recommendation 5

The CIO should

(a) Update NARA's password requirements to include the requirements detailed in NIST SP 800-68 and FDCC settings.

(b) Implement FDCC password requirements for NARA desktops.

Management Comment(s)

Management did not concur with recommendation. Management suggested rewording the recommendation to state NARA should re-evaluate its current password policy and conduct a risk assessment of the impact of modifying its current policy to match FDCC settings.

OIG Response to Management Response

We do not concur that management should re-evaluate its current password policy and conduct a risk assessment. Our recommendation reflects the OMB mandated FDCC password requirements. According to an OMB official, OMB expects 100 percent compliance and if an agency is not compliant, they should have to plan to get to full FDCC compliance.

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: AUG 19 2008

To: Office of Inspector General (OIG)

From: Office of Information Services (NH)

Subject: Comments on Draft Report 08-10: Audit of NARA's Implementation of the Federal Desktop Core Configuration

We thank you for the opportunity to review and comment on the subject draft report, as well as for meeting with us on August 7th and making agreed-upon changes to the report. As we discussed at the meeting, what follows are our comments on each of the recommendations and the current status of our FDCC implementation. While we acknowledge the "snapshot in time" for this and other performance audits, we do hope the OIG will note and acknowledge the progress we have made since the field work was completed for this audit earlier this year.

Our Office continues to work diligently to comply with this and other OMB mandates to secure all our IT systems to ensure reliability, integrity, and availability of NARA information resources. Please call me at any time to discuss our IT program for this and any other issue.

Technical questions about the status of our FDCC implementation can be directed to
—— b(6) —— or —— b(6) ——

Martha Morphy

MARTHA MORPHY
Assistant Archivist for Information Services

COMMENTS ON OIG DRAFT REPORT 08-10: AUDIT OF NARA'S IMPLEMENTATION OF THE FEDERAL DESKTOP CORE CONFIGURATION

Recommendation 1 - Management Comment(s): We concur with the recommendation. Both items (a) and (b) have already been completed. RFC 1601 (provided to the auditor) includes the history of work that has occurred to meet both of these recommendations.

Recommendation 2 - Management Comment(s): We concur with the recommendation, provided NIST or OMB allow for any explanations to be provided with future submissions related to FDCC. However, the desktop environment currently is much different than what was current at the end of March 2008. If the recommendation is to provide a disclaimer regarding the March submission to NIST, and not what is current at the time of the next status report, then this can be done provided there is the ability to provide additional explanations with the submission.

Recommendation 3 - Management Comment(s): We concur with the recommendation. As stated under recommendation 1 above, implementation and test plans have already been developed and FDCC settings (minus deviations) have already been pushed to desktops enterprise-wide. RFC 1601 includes the history of work that has occurred to meet this recommendation.

Recommendation 4 - Management Comment(s): We concur with the recommendation. The remaining FDCC deviations have been individually added to the "NARANET GSS Desktops" Plan of Action and Milestones (POA&M).

Recommendation 5 - Management Comment(s): The recommendation as currently worded does not fit in with NARA's plans to address the password-related FDCC deviations on the agency's desktops. As such, we do not concur with this recommendation as it is currently constructed. We would suggest that the recommendation be re-worded to state that NARA will re-evaluate its current password policy and conduct a risk assessment of the impact of modifying its current policy to match FDCC settings.

The password settings that deviate from FDCC settings have been added to the NARANET GSS Desktops POAM, where they will be evaluated and tracked. Five of the current deviations are related to password settings. As part of re-evaluating the current password settings and possibly changing them to match the FDCC, NARA would need to implement these same settings within

high b(2)