AUDIT OF NARA'S CHANGE CONTROL PROCESS

OIG Report No. 09-09

May 11, 2009

EXECUTIVE SUMMARY

The National Archives and Records Administration (NARA) Office of Inspector General (OIG) completed an audit of NARA's Change Control Process. Change Control is a formal process used to ensure that changes to Information Technology (IT) systems are introduced in a controlled and coordinated manner and are assessed and approved by management before their implementation. During the audit, we assessed the process to determine whether NARA authorizes, documents, tests, and controls changes to their information systems. To accomplish our review, we selected nine operational systems, which had recent system changes and/or supported NARA's core mission. For each of these systems, we evaluated a sample of system changes.

To adequately manage the change control process, NARA must put controls in place to prevent, detect, and correct unauthorized or unintended changes to their information systems. According to the National Institute of Standards and Technology (NIST), a change control process should involve a systematic proposal, justification, implementation, test/evaluation, review, and disposition of all changes to an information system.

Our review found that NARA did not authorize, document, test, and control all changes to their information systems. Specifically, we found NARA did not always

- Authorize or document all system changes;
- Complete security impact analysis prior to approving and implementing changes;
- Fully test changes prior to implementation;
- Adequately manage and control emergency changes; and
- Employ automated mechanisms to document proposed changes to high impact[1] systems.

A formalized and rigorously enforced change control process brings uniformity and structure to the function. Ultimately, this very process serves to ensure conformity with NIST guidance and most importantly protect the integrity and content of IT systems and the data residing upon them. Conversely, a decentralized, laissez-faire approach may adversely impact an organization, such as NARA.

Establishing controls over the modification of information systems helps to ensure that only authorized programs and authorized modifications are implemented. Without proper controls, there is a risk security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced. This places NARA at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Also, without a formal review process, rapid changes to information systems could result in unforeseen technical problems or the use of inadequate risk analysis and testing. Finally, weaknesses in the change control process

[1] A high impact system is an information system in which at least one security objective (confidentiality, integrity, and availability) is rated as high.

could limit NARA's ability to effectively protect the confidentiality, integrity, and availability of its systems and information.

We made nine recommendations that when implemented will improve NARA's change control process and enhance the security of NARA information systems.

BACKGROUND

Federal Information Processing Standards Publication (FIPS PUB) 200, *Minimum Security Requirements for Federal Information and Information Systems*, specifies minimum security requirements for federal information systems. FIPS PUB 200 directs federal agencies to meet the minimum security requirements through the use of the security controls outlined in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. One of the controls outlined in NIST SP 800-53 is configuration change control, which involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades, and modifications.

The selection of appropriate security controls is a risk-based activity that should take into consideration the security categorization (i.e. High, Moderate, and Low) of each information system. For example, systems identified as high impact should have more stringent controls than systems identified as low impact. NIST SP 800-53 provides different levels of controls for each categorization, such as the supplemental guidance and control enhancements for moderate and high risk systems. FIPS 200 also requires organizations to develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in FIPS 200 and must ensure their effective implementation.

NARA has developed various levels of guidance, polices, and procedures relating to change controls. For instance, the Enterprise Architecture (EA) Configuration Management Procedures specifies the procedures used to establish, modify, and manage all EA work products. In addition, NARA's System Development Lifecycle directive includes Configuration Management Guidelines for the implementation and maintenance of NARA IT systems. Finally, NARA's IT Security Policy states that for moderate or high integrity information systems, NARA:

- Monitors changes to each information system and conducts security impact analyses to determine the effects of the changes.
- Approves individual access privileges and enforces physical and logical access restrictions associated with change to each information system and generates, retains, and reviews records reflecting all such changes.

Prior audit reports and reviews have identified weaknesses in NARA's configuration management. Since 2004, weaknesses in Configuration Management have been identified as a reportable condition on the each of the annual audits of NARA's Financial Statements. Some of these weaknesses were related to NARA's Change Control Process. In particular, proper approvals were not obtained for changes to NARANet and the Records Center Program Billing System (RCPBS). Also, a review conducted by Science Applications International Corporation (SAIC), found that while NARA policies provide guidance on management, operational, and technical security mechanisms, they are neither comprehensive nor specific enough to NARA to be measurable or enforceable. In addition, NARA policies are only partially implemented.

The responsibilities associated with NARA's Change Control Process mainly fall under the Office of Information Services (NH). Specifically, the Information Technology Services Division (NHT) is responsible for coordinating and implementing upgrades and enhancements to NARA's existing infrastructure and the System Development Division (NHV) helps develop major enhancements of information technology (IT) applications and systems. In addition, some system owners outside of NH are responsible for managing their system's Change Control Process.

OBJECTIVE, SCOPE, METHODOLOGY

The objective of this audit was to determine whether NARA authorizes, documents, tests, and controls changes to its information systems. Specifically, we determined whether the NARA change control process included (a) documenting, approving, testing, and reviewing of system changes; (b) security impact analysis; and (c) adequate management and control of emergency changes.

We examined applicable laws, regulations, NARA guidance, and other IT-related guidance, including (a) FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems*; (b) NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*; (c) NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*; (d) Government Accountability Office (GAO) *Federal Information System Controls Audit Manual*; (e) NARA 812, *Enterprise Architecture*; and (f) NARA 805, *Systems Development Lifecycle*.

To accomplish our objective, we reviewed NARA's change control activities and documentation and selected a sample of information systems to perform detailed audit tests. We reviewed nine[2] operational NARA systems, which had system changes during the six month period prior to audit field work and/or directly supported NARA's mission. For each of these systems, we selected a judgmental sample of system changes to review. This sample included 52 system changes. We also met with system owners and other officials involved in the change control process. The review of the selected systems and system changes allowed us to conduct a program level review of NARA's change control process.

Our audit work was performed at Archives II in College Park, MD between June 2008 and December 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.

[2] See Attachment I for a list of systems reviewed.

FINDINGS AND RECOMMENDATIONS

System Changes Not Always Documented and Approved

NARA has not authorized and documented all changes to their information systems. This condition occurred because NARA has an informal and decentralized change control process. In addition, some NARA policies and procedures are outdated. By not authorizing and documenting changes, there is a risk that unauthorized programs and modifications could be implemented or security features could be unknowingly altered.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, requires agencies to authorize, document, and control changes to information systems. To meet this requirement, NIST SP 800-53 provides supplemental guidance, which states the organization should manage changes using an organizationally approved process, such as a chartered Configuration Control Board (CCB). The supplemental guidance also states that configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review and disposition of changes to the information system, including upgrades and modifications.

However, we found that NARA has not authorized and fully documented all changes to their information systems. For example, approvals were not documented for over 63% (33 of 52) of the change requests reviewed. In some instances, the documentation of approval was not included in their change control procedures. In addition, some of the changes were not fully documented. For instance, one system maintained their list of changes in Microsoft Excel. However, this list provided limited detail or information regarding each change.

This occurred because NARA has a decentralized change control process with varying degrees of formality. For instance, the Network and Infrastructure Systems CCB reviews and approves changes that affect NARANet, whereas individual application CCBs review and approve application changes. These application CCBs have different change control protocol and procedures. For example, some system changes[3] are approved during CCB meetings and are not documented in a formal change request form. The use of a standardized change request form helps ensure requests are clearly communicated and approvals are documented. In other cases, the change request documentation indicated CCB approval was not needed. These reasons included:

- A member of the Technical Review Board determined that the change did not require CCB approval.
- The requested change was a critical security related issue and was automatically granted CCB approval.

Consequently, approvals of NARA system changes were not always documented.

In addition, four of the systems reviewed (AERIC, CMRS, PERL, and PPMS) had not developed or documented sufficient change control procedures. . In some cases[4], a CCB

[3] This was noted for the eDOCS and AERIC systems.
[4] This was noted in the charters for CMRS, PERL, and PPMS.

charter or plan was developed; however, it did not fully address change control policies and procedures, such as who can authorize a modification and how these authorizations should be documented. When asked why a Configuration Management Plan was not developed, one system manager stated a determination was made that procedures were not needed. However, during audit fieldwork, the contractor was tasked by management with developing a Configuration Management Plan for that system

Finally, some confusion may be attributed to the use of an older NIST Handbook. Specifically, in the IT Security Mechanisms document of NARA's Enterprise Architecture, it states that NARA's configuration management will be based on NIST SP 800-12[5], *An Introduction to Computer Security*, which describes configuration management as the process of keeping track of changes to the system, and if needed, approving them. However, NIST considers this publication to be a broad overview of computer security that discusses the benefits of various security controls. Although useful to learn the basics of computer security, this document was written in 1995 and does not specify requirements or describe the detailed steps necessary to implement a computer security program.

Establishing controls, such as adequate documentation and approvals, over the modification of application software programs helps to ensure only authorized programs and authorized modifications are implemented. Without proper controls, there is also a risk that security features could be inadvertently or deliberately omitted or "turned off" or that processing irregularities or malicious code could be introduced.

Recommendation 1

We recommend the CIO enforce a more formal and centralized change control process.

Recommendation 2

We recommend the CIO ensure all systems have adequate and documented change control procedures.

Management Comment(s)

Management concurred with the recommendations.

[5] NIST 800-53, *Recommended Security Controls for Federal Information System*, provides more comprehensive and updated recommendations for change controls.

Security Analysis Not Conducted

NARA did not always complete or document the security impact analysis prior to approving and implementing changes to their information systems. This occurred because NARA's change control procedures and guidance do not require a security analysis. Also, the Request for Change (RFC) form[6] does not include a space to document adjustments or potential impacts to security resulting from the proposed change. Without a security impact analysis, changes could be introduced into NARA systems that increase the risk of a security incident.

We found that NARA did not always complete or document the security impact analysis prior to approving and implementing changes to their information systems. Specifically, in our review of 52 change requests, at least 44 were approved without any documented review of a security impact analysis. These change requests were for systems rated as moderate or high impact systems and these weaknesses were noted for each of the nine systems reviewed.

For systems classified as Moderate and High impact, NIST SP 800-53 requires that approvals to implement a change to an information system include successful results from the security analysis of the change. Also, NARA's Enterprise Architecture IT Security Policy states that NARA conducts security impact analyses to determine the effects of system changes for moderate or high integrity systems. However, NARA's change control procedures and guidance do not require security analysis prior to implementing changes. NARA's Configuration Management Procedures and Systems Development Guidelines only require an impact assessment, which includes changes in scope, cost, schedule, resource needs and integration ramifications. Security is not included as a requirement of this impact assessment. Management stated that this was an oversight in the policy.

Further, the RFC form that most systems use to document system changes does not include a space to document adjustments or potential impacts to security resulting from the proposed change. The Information Technology Operations Chief agreed that security impact could be added to the RFC form.

Some system owners stated that not all changes affect system security and if there had been any security related changes, the IT Security Staff (NHI) would have been contacted. However, such information was not noted in the documentation of system changes for systems such as CMRS, AERIC, and ARC.

Management agreed that a formal security impact analysis was not part of their change control process. Impacts to security are usually considered before implementing system changes, but are not always documented. Instead, a member of NHI generally attends the CCB meetings and is aware of some system changes. We were also informed that within

[6] The Request for Change form is used to track and manage system changes requiring formalized assessments and approvals. This form is used for changes reviewed and approved by the Network Infrastructure CCB.

the last year the Security Operations Manager was included in NARANet system change reviews. We found he had reviewed at least two system changes included in the sample. However, this does not adequately fulfill the requirement for a security impact analysis.

Changes to an information system can have a significant impact on the security of the system. Documenting information system changes and assessing the potential impact on the security of the system is an essential aspect of maintaining the security posture. An effective control policy and associated procedures are essential to ensuring adequate consideration of the potential security impact of specific changes to a system.

Without a security impact analysis, changes could be introduced into NARA systems that increase the risk of a security incident. By not documenting or requiring a security analysis, NARA lacks assurance that proposed changes could adversely affect IT system security.

Recommendation 3

We recommend the CIO enforce and if necessary update NARA procedures to require security analysis prior to implementing system changes and provide guidance for when a security analysis is warranted.

Recommendation 4

We recommend NHT modify the Request for Change (RFC) form to include a space to document adjustments or potential impacts to security.

Management Comment(s)

Management concurred with the recommendations.

Inadequate Testing of Changes

NARA did not adequately test all changes prior to introducing them into IT systems as suggested by Federal regulations. This occurred because of a lack of guidance regarding the testing of system changes. Inadequate testing can have a significant impact on system data reliability and availability.

According to NIST SP 800-53 adequate configuration change control involves systematic testing of system changes. The Federal Information System Controls Audit Manual (FISCAM), states that a disciplined process for testing and approving new and modified programs prior to their implementation is essential to make sure programs operate as intended and that no unauthorized changes are introduced. The extent of testing varies depending on the type or extent of the proposed modification.

A detailed test plan should be developed for each modification defining the levels and types of tests to be performed. Because testing is an iterative process, it is important to adhere to a formal set of procedures or standards. All test data, transactions, and results should be saved and documented to facilitate future testing of other modifications and allow a reconstruction if future events necessitate a revisit of the actual tests and results. Also, test plans should be approved by all responsible parties.

However, we found that NARA did not adequately test all changes prior to implementation. Specifically, test plans were not developed or maintained for 31 of the 52 system changes reviewed. Weaknesses were noted in all but one (ADRRES) of the systems reviewed. In many instances, the RFC form, which requires a complete listing of all steps and tests to be performed to assure that the intended results of the change have been achieved, simply stated "to be determined". When asked for these test plans, none were provided. In some cases, it was the responsibility of the contractor to develop such test plans, but none were developed or could be provided. A contractor monitoring process is in place; however, when a deficiency is noted, follow up is not always completed to ensure the contractor corrects the problem.

NARA also lacked documentation and assurance that testing was completed prior to introducing the system change into the production environment. Documented test results could only be provided for three[7] of the 52 system changes reviewed.

When asked why test plans and results were not documented, some system owners stated that change requests were of low complexity and did not need a formalized test plan. However, this was not documented in the request documentation. Additionally, some systems do not have a test environment; therefore, testing cannot be done prior to implementing the change into the production environment. Also, some changes can only be testing once it has been placed into production and not prior. Consequently, a backup plan or a rollback plan is developed, in case problems are encountered during the implementation. Finally, there appears to be limited guidance on developing test plans and documenting or maintaining the test results.

Minor modifications may require less extensive testing; however, changes should still be carefully controlled and approved since relatively minor program code changes, if done incorrectly can have a significant impact on overall data reliability and availability. For example, in the system changes reviewed, at least two that were inadequately tested caused a delay or disruption for system users. By not adequately testing changes prior to implementation, NARA takes a chance that changes introduced to its systems could adversely affect security and data.

Recommendation 5

We recommend that the CIO require the test plans and test results to be documented and maintained.

[7] The three changes were for the ADRESS/URTS, CMRS, and NARANet systems.

Recommendation 6

We recommend that the CIO develop guidance to aid in

- Developing test plans;
- Determining if a test plan is required and how to, document the decision if one is not required; and
- Maintaining the test results.

Management Comment(s)

Management concurred with the recommendations.

Emergency Changes Not Adequately Controlled

NARA did not adequately manage and control emergency or urgent changes to their information systems as required by NIST. This condition occurred because NARA has not established or mandated any additional controls for emergency change procedures. Due to the critical nature of emergency changes, additional controls are needed to reduce the risk of suspending or abbreviating normal controls and to prevent disruptions to IT systems.

During our review, we found that NARA does not adequately manage and control emergency or urgent changes. For instance, emergency change procedures have not been developed or documented for all NARA information systems. Of the nine systems reviewed, only three (ARC, ENOS, and NARANet) had additional procedures for emergency changes. It is important to follow established procedures for emergency changes to reduce the risk of suspending or abbreviating normal controls. For most systems reviewed, post-emergency reviews were not required and consequently were not conducted for all emergency changes. As a result, additional controls are not in place for emergency changes.

Furthermore, similar to non-emergency changes, approval of change requests was not always documented and sufficient testing and security analysis was not conducted prior to implementation. In particular, we noted these weaknesses for the following systems: AERIC, ARC, eDOCS, ENOS, NARANet, and PERL.

For systems classified as Moderate and High, NIST SP 800-53 requires that the organization include emergency changes in the configuration change control process, including changes resulting from the remediation of system flaws. In addition, the FISCAM states that emergency procedures should specify the following:

- When emergency software changes are warranted;
- Who may authorize emergency changes;

- How emergency changes are to be documented; and
- Within what period after implementation the change must be tested and approved.

FISCAM also states logs of emergency changes and related documentation should be periodically reviewed by data center management or security administrators to determine whether all such changes have been tested and received final approval.

NARA has not established or mandated any additional controls for emergency change procedures. Specifically, NARA policies, procedures, and guidance related to change controls do not address emergency changes. We found three systems with procedures for emergency changes. However, NARA did not require system owners or project managers to develop or document additional control procedures related to emergency changes.

When asked about emergency changes, most system owners and project managers stated that their systems did not have emergency changes and therefore, felt that emergency change procedures were not necessary. However, due to the critical nature of emergency changes, additional controls are needed to reduce the risk of suspending or abbreviating normal controls. Pressure to make rapid changes to systems without a formal review process often result in a critical system failure due to unforeseen technical problems.

Recommendation 7

We recommend

(a) CIO strengthens system change control policies and procedures to include emergency change control procedures.

(b) System owners implement additional procedures to control emergency changes.

Management Comment(s)

Management concurred with the recommendations.

Automated Mechanisms Not Always Used

NARA does not always employ automated mechanisms to document proposed changes to High impact systems. This occurred because NARA does not require all systems or all systems categorized as High impact, to use PVCS Tracker or another automated mechanism to manage system changes. Without these mechanisms, NARA High impact systems are not as secure and there is an increased risk of unauthorized changes.

For systems categorized as High impact, NIST SP 800-53 requires organizations to employ automated mechanisms to (a) document proposed changes to information systems; (b) notify appropriate approval authorities; (c) highlight approvals that have not been received in a timely manner; (d) inhibit change until necessary approvals are received; and (e) document completed changes to the information system.

NARA does not always employ automated mechanisms to document proposed changes to High impact systems. Specifically, automated mechanisms to document proposed and completed changes were not employed for three NARA systems (AERIC, eDOCS, and PERL) categorized as High impact. Instead, these systems use non-automated mechanisms, such as meeting notes and Excel spreadsheets.

This occurred because NARA does not require or enforce all systems or all systems categorized as High impact, to use PVCS Tracker or another automated mechanism to manage system changes. In some cases, automated mechanisms may not be cost effective for systems that do not have major system enhancements, such as AERIC. However, if automated mechanisms are not employed, additional controls should be in place to prevent unauthorized changes. These controls include restricting access to implementing changes and reviewing access logs to ensure unapproved changes are not occurring.

Automated mechanisms can notify appropriate approval authorities; highlight approvals that have not been received in a timely manner; and inhibit change until necessary approvals are received. Without these mechanisms, NARA High impact systems are not as secure and there is an increased risk of unauthorized changes.

Recommendation 8

We recommend the CIO either require systems categorized as High impact to use an automated system (such as PVCS Tracker) or implement additional controls.

Management Comment(s)

Management concurred with the recommendation.

ATTACHMENT 1: NARA Systems Reviewed

System Acronym	Full Name	Description	Impact Level	System Changes Reviewed	Documentation and Approval Weaknesses	Security Analysis Weaknesses	Testing Weaknesses
ADRRES	Archival Declassification Review and Redaction System	Automates the process of reviewing and redacting sensitive and classified materials	High	1		X	
AERIC	Archival Electronic Records Inspection and Control	Preserves the logical structure of databases, and verifies that the records received are those supported by the accompanying documentation	High	8	X	X	X
ARC	Archival Research Catalog	Online catalog of NARA holdings	Moderate	3	X	X	X
CMRS	Case Management and Reporting System	Provides workload management and processes to fulfill requests for military records	High	4		X	X
eDOCS	Electronic Document Management System	Automates the creation of the daily Federal Register	High	9	X	X	X
ENOS/ Order Online	Expanding NARA Online Services	Supports ordering and fulfilling of selected records reproductions online	Moderate	7	X	X	X
NARANet	NARA Network	Primary general support system, providing standard desktop applications and Internet access to NARA staff	High	12	X	X	X
PERL	Presidential Electronic Records Library	Used to ingest and provide internal access to the Presidential electronic records	High	4		X	X
PPMS	Personal Property Management System	Provides property asset management for all NARA's personal property	Moderate[8]	4	X	X	X

[8] PPMS was categorized as "Low" on the system inventory; however, the revised Contingency Plan (dated August 22, 2008) rates the system as "Medium" for data integrity. Using the high water method described in FIPS 199, we consider this system to be Moderate.

Appendix A

National Archives and Records Administration

8601 Adelphi Road
College Park, Maryland 20740-6001

Date: MAY 5 2009

To: Office of the Inspector General (OIG)

From: Office of Information Services (NH)

Subject: Revised Draft Report 09-09, Audit of NARA's Change Control Process

We have reviewed the revised draft OIG Report No. 09-09, March 10, 2009, titled *Audit of NARA's Change Control Process*. We want to thank the auditor for meeting with NH staff to discuss the first set of comments sent to OIG on April 10, 2009. The changes that were made to the report following the meeting have resulted in our accepting the recommendations as written, or, in some cases, revised as agreed to in the meeting. We have copied the recommendations on the following pages and provide our concurrence on them individually. If we have incorrectly copied the updated text from the revised report e-mailed to us on April 29, 2009, please let us know.

Please thank Christine Dzara for working with us on revision to the original draft, and we look forward to working with her on developing an acceptable action plan once we receive the report in final. If you have any questions about our response, please call me or Steve Heaps on 837-3170.

Martha Morphy

MARTHA MORPHY
Assistant Archivist for Information Services

Recommendation 1: We recommend the CIO enforce a more formal and centralized change control process.

We concur with the recommendation.

Recommendation 2: We recommend the CIO ensure all systems have adequate and documented change control procedures.

We concur with the recommendation.

Recommendation 3: We recommend the CIO enforce and if necessary update NARA procedures to require security analysis prior to implementing system changes and provide guidance for when a security analysis is warranted.

We concur with the recommendation.

Recommendation 4: We recommend NHT modify the Request for Change (RFC) form to include a space to document adjustments or potential impacts to security.

We concur with the recommendation.

Recommendation 5: We recommend that the CIO require the test plans and test results to be documented and maintained.

We concur with the recommendation.

Recommendation 6: We recommend that the CIO develop guidance to aid in

- **Developing test plans;**
- **Determining if a test plan is required and how to, document the decision if one is not required; and**
- **Maintaining the test results.**

We concur with the recommendation.

Recommendation 7: We recommend:

(a) CIO strengthen system change control policies and procedures to include emergency change control procedures.

(b) System owners implement additional procedures to control emergency changes.

We concur with the recommendation.

Recommendation 8: We recommend the CIO either require systems categorized as High impact to use an automated system, such as PVCS Tracker, or implement additional controls.

We concur with the recommendation.