Systems Evaluation of the Agencywide Document Access and Management System

OIG-04-A-21 September 30, 2004

REDACTED FOR PUBLIC RELEASE

OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

System Evaluation of the
Agencywide Documents Access and
Management System

OIG–04-A-21   September 30, 2004

EVALUATION REPORT

All publicly available OIG reports (including this report) are accessible through NRC's website at:
http://www.nrc.gov/reading-rm/doc-collections/insp-gen/

September 30, 2004

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

FROM: Stephen D. Dingbaum**/RA/**
Assistant Inspector General for Audits

SUBJECT: SYSTEM EVALUATION OF THE AGENCYWIDE DOCUMENTS ACCESS AND MANAGEMENT SYSTEM (ADAMS) (OIG-04-A-21)

This evaluation was conducted as part of the Office of the Inspector General's review of NRC's implementation of the Federal Information Security Management Act (FISMA) for FY 2004. Richard S. Carson & Associates, Inc., performed this independent system evaluation on behalf of OIG.

Based on its review and evaluation of ADAMS' management, operational, and technical controls, Richard S. Carson & Associates, Inc., determined that ADAMS has the following weaknesses:

- Security documentation does not always follow required guidelines.
- Security protection requirements are inconsistent within ADAMS' security documentation.
- NRC is not tracking all action items resulting from testing the security controls.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on September 15, 2004, NRC officials provided comments concerning the draft audit report and opted not to submit formal written comments to this report.

If you have any questions or wish to discuss this report, please call me at 415-5915 or Beth Serepca at 415-5911.

Attachment: As stated

Distribution List

B. John Garrick, Chairman, Advisory Committee on Nuclear Waste
Mario V. Bonaca, Chairman, Advisory Committee on Reactor Safeguards
John T. Larkins, Executive Director, Advisory Committee on Reactor
  Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and
  Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
Dennis K. Rathbun, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
Patricia G. Norry, Deputy Executive Director for Management Services, OEDO
William F. Kane, Deputy Executive Director for Homeland Protection
  and Preparedness, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research
  and State Programs, OEDO
Ellis W. Merschoff, Deputy Executive Director for Reactor Programs, OEDO
William M. Dean, Assistant for Operations, OEDO
Jacqueline E. Silber, Chief Information Officer
Michael L. Springer, Director, Office of Administration
Frank J. Congel, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Paul E. Bird, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV
Office of Public Affairs, Region I
Office of Public Affairs, Region II
Office of Public Affairs, Region IV

"Office of the Inspector General
System Evaluation of the
Agencywide Documents Access and Management System
(ADAMS)"

Contract Number: GS-00F-0001N
Delivery Order Number: DR-36-03-346

September 24, 2004

"The views, opinions, and findings contained in this report are those of the authors and should not be construed as an official U.S. Nuclear Regulatory Commission position, policy, or decision, unless so designated by other official documentation."

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347), which includes the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an independent evaluation of an agency's information security program and practices, and an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. As part of the Fiscal Year 2004 FISMA independent evaluation of the U.S. Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the Agencywide Documents Access and Management System (ADAMS).

ADAMS is an electronic record keeping system that has been approved by the National Archives and Records Administration. NRC processes hundreds of legal, administrative, and regulatory documents each day. These documents are generated both internally and externally in various formats and are made available, in whole or in part, to the Government or the public, for reference and reuse. NRC developed ADAMS to replace the paper-oriented environment that no longer supported its needs.

PURPOSE

The system evaluation objectives were to review and evaluate the management, operational, and technical controls for ADAMS.

RESULTS IN BRIEF

Carson Associates reviewed ADAMS security documentation and found that ADAMS security documentation is not always consistent with National Institute of Standards and Technology (NIST) guidelines, the security protection requirements are inconsistent within ADAMS security documentation, and findings and recommendations resulting from testing are not consistently being tracked. None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in Office of Management and Budget guidance.

<u>Security Documentation Is Not Always Consistent With NIST Guidelines</u>

FISMA directs the Secretary of Commerce, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to Federal information systems. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans. NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, which was revised in September 2003, states that NRC shall comply with NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, risk assessments, and contingency plans), and other applicable NIST guidance for information technology security processes, procedures, and testing.

The previous version of MD 12.5 did not require compliance with NIST guidelines, however, Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, states that each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management. OMB periodically reminds agencies that agency security practices should be consistent with NIST guidance. The FY 2004 FISMA guidance issued by OMB specifically states that agencies must follow NIST standards and guidance. Use of NIST guidance is flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance.

Carson Associates reviewed the ADAMS Risk Assessment, Security Plan, and Business Continuity Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

Security Protection Requirements Are Inconsistent Within Security Documentation

FISMA defines the term "information security" to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability is ensuring timely and reliable access to and use of information. Confidentiality, integrity and availability are often referred to as security protection requirements or security objectives for a system. The security protection requirements defined in the ADAMS Security Plan and in the FY 2003 and FY 2004 ADAMS self-assessments are inconsistent.

Findings and Recommendations Resulting From Testing Are Not Consistently Being Tracked

The FY 2003 FISMA independent evaluation of NRC's information security program found that not all corrective actions resulting from security reviews and testing were being tracked and that the agency's corrective action process needed improvement. The Office of the Inspector General (OIG) recommended that the agency identify all weaknesses and recommendations from security documentation and any other security reviews, and determine in which tool the recommendations will be tracked. In November 2003, the Office of the Chief Information Officer (OCIO) issued a memo describing the agency's information technology security action item tracking process, strategy, and tools. Carson Associates found that findings and recommendations resulting from testing of ADAMS security controls and from ADAMS contingency plan testing are not consistently being tracked.

RECOMMENDATIONS

This report makes six recommendations to the Executive Director for Operations to strengthen management, operational, and technical controls for ADAMS. A consolidated list of recommendations appears on page 13 of this report.

AGENCY COMMENTS

On September 15, 2004, the Executive Director for Operations provided comments concerning the draft system evaluation report. We modified the report as we determined appropriate in response to these comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Documents Access and Management System
BCP	Business Continuity Plan
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GISRA	Government Information Security Reform Act
ITSSTS	Information Technology Systems Security Tracking System
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication

[Page intentionally left blank]

TABLE OF CONTENTS

Appendices

[Page intentionally left blank]

1 Background

On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347), which includes the Federal Information Security Management Act (FISMA) of 2002[1]. FISMA outlines the information security management requirements for agencies, which include an independent evaluation of an agency's information security program and practices, and an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. As part of the Fiscal Year 2004 FISMA independent evaluation of the U.S. Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the Agencywide Documents Access and Management System (ADAMS).

Agencywide Documents Access and Management System

ADAMS is an electronic record keeping system that has been approved by the National Archives and Records Administration. NRC processes hundreds of legal, administrative, and regulatory documents each day. These documents are generated both internally and externally in various formats and are made available, in whole or in part, to the Government or the public, for reference and reuse. NRC developed ADAMS to replace the paper-oriented environment that no longer supported its needs. ADAMS provides the basis for modernizing the legacy document reference searching and microfiche retrieval system, for automating manual document handling processes, and for consolidating various office based systems into one central system for document capture, storage, control, and dissemination. ADAMS provides the capability for staff to collaborate on and track the progress of documents in preparation, store all documents electronically in one location, capture documents as they are created, and allow staff to search the electronic document collection and the index of the existing historical collection at their workstations.

The NRC Office of the Chief Information Officer (OCIO) is the ADAMS system owner. The system is categorized as a Major Application[2] and is in the operational[3] phase of its life cycle.

System Evaluation Process

ADAMS was evaluated by reviewing system documentation maintained by OCIO. As recommended by the Office of Management and Budget (OMB), Carson Associates reviewed the following documents for adherence to standards and consistency with guidelines issued by the National Institute of Standards and Technology (NIST).

[1] The Federal Information Security Management Act of 2002 was enacted on December 17, 2002, as part of the E-Government Act of 2002 (Public Law 107-347), and replaces the Government Information Security Reform Act, which expired in November 2002.

[2] An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[3] A system's life cycle typically comprises five phases: initiation, development/acquisition, implementation, operation/maintenance, and disposal. In the operation/maintenance phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.

- ADAMS Risk Assessment, March 2002
- ADAMS Security Plan, June 2002
- ADAMS Business Continuity Plan, June 2002 and a revised draft from May 2004
- ADAMS Security Test and Evaluation Plan and Report, June 2002
- Certification and Accreditation Statement, July 2002
- Mitigation Plan, July 2002
- Privacy Impact Assessment
- FY 2003 and draft FY 2004 ADAMS Self-Assessment

The documents were reviewed to determine whether they are consistent with NIST guidance and whether they describe the management[4], operational[5], and technical[6] controls in place for ADAMS.

2 Purpose

The system evaluation objectives were to review and evaluate the management, operational, and technical controls for ADAMS.

3 Findings

Carson Associates reviewed ADAMS security documentation and found that:

- ADAMS security documentation is not always consistent National Institute of Standards and Technology guidelines.
- Security protection requirements are inconsistent within ADAMS security documentation.
- Findings and recommendations resulting from testing are not consistently being tracked.

None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in Office of Management and Budget guidance.

3.1 Security Documentation Is Not Always Consistent With NIST Guidelines

FISMA directs the Secretary of Commerce, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to Federal information systems. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans. NRC Management Directive (MD) 12.5, *NRC*

[4] The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
[5] The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
[6] The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

Automated Information Security Program, which was revised in September 2003, states that NRC shall comply with NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, risk assessments, and contingency plans), and other applicable NIST guidance for information technology security processes, procedures, and testing.

The previous version of MD 12.5 did not require compliance with NIST guidelines, however, OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, states that each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce[7], the General Services Administration and the Office of Personnel Management. OMB periodically reminds agencies that agency security practices should be consistent with NIST guidance. The FY 2004 FISMA guidance issued by OMB[8] specifically states that agencies must follow NIST standards and guidance. Use of NIST guidance is flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance.

Carson Associates reviewed the ADAMS Risk Assessment, Security Plan, and Business Continuity Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

ADAMS Risk Assessment Report Is Not Consistent With NIST Guidelines

The Final ADAMS Risk Assessment Report, dated March 25, 2002, states that the methodology used to conduct the risk assessment was "based on guidance provided in NIST Special Publication (SP) 800-30, *Risk Management Guide*."[9] However, the Risk Assessment Report is not consistent with the referenced NIST document. Specifically, the Risk Assessment Report (1) does not describe the threat-sources and vulnerabilities identified for ADAMS, and (2) does not describe how risk levels were determined.

NIST SP 800-30 describes risk as "a function of the likelihood of a given threat-source's[10] exercising a particular potential vulnerability,[11] and the resulting impact of that adverse event on the organization." The risk assessment methodology described in NIST SP 800-30 encompasses nine primary steps. Step 2 is threat identification, and Step 3 is vulnerability identification. The output from Step 2 is a threat statement containing a list of threat-sources that could exploit

[7] NIST is part of the Technology Administration within the Department of Commerce.

[8] OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, dated August 23, 2004.

[9] While the cover of NIST SP 800-30 indicates it was published in July 2002, the document was first published in its current form in January 2002.

[10] A threat-source is either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

[11] The potential for a particular threat-source exercise (accidentally trigger or intentionally exploit) a particular vulnerability is also known as a threat. A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

system vulnerabilities. The output from Step 3 is a list of the system vulnerabilities that could be exercised by the potential threat-sources. Each threat-source/vulnerability pair identifies a potential threat to the system.

The ADAMS Risk Assessment Report presents a table summarizing the findings and recommendations. The second column of the table is labeled “Risk”, when in fact; the data in this column represent threats. The ADAMS Risk Assessment Report does not include a list of potential threat-sources that could exploit system vulnerabilities, does not include a list of potential vulnerabilities applicable to the system, and does not discuss the threat-source/vulnerability pairs that identified the threats listed in the summary table.

NIST SP 800-30 describes Steps 5 and 6 of the risk assessment methodology as likelihood determination and impact analysis. Step 7 is risk determination, which is a function of the likelihood of a given threat-source’s attempting to exercise a given vulnerability (i.e., the likelihood of the threat), the magnitude of the impact should a threat-source successfully exercise the vulnerability (i.e., the impact of the threat), and the adequacy of planned or existing security controls for reducing or eliminating risk. To measure risk, a risk scale and risk-level matrix must be developed.

In the ADAMS Risk Assessment Report, the fourth column of the table summarizing the findings and recommendations is labeled “Level of Risk” and contains values of either “High,” “Medium,” or “Low.” However, the ADAMS Risk Assessment Report does not identify or describe how these risk levels were determined. According to the risk-level matrix presented in NIST SP 800-30, a threat identified as having a “Medium” risk level could mean either:

- The threat has a high likelihood and a medium impact
- The threat has a medium likelihood and a medium impact
- The threat has a medium likelihood and high impact

The ADAMS Risk Assessment Report identifies several threats with a “Medium” risk level, but does not describe whether these were threats with high impact or a high likelihood. The controls recommended to mitigate the risk could vary greatly depending on which factor (likelihood or impact) contributed the most to the risk level. Understanding likelihood and impact is also important in prioritizing the implementation of recommended corrective actions. If the agency must choose between which medium risk to mitigate first, the agency might want to address the risk with the high impact first.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Update the ADAMS Risk Assessment Report to be consistent with National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide*.

ADAMS Security Plan Does Not Describe All Security Controls Identified As In-Place

OMB A-130 states that security plans shall be consistent with guidance issued by NIST. NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that the purpose of a security plan is to provide an overview of the security requirements of the system and describe controls in place or planned for meeting those requirements. NIST SP 800-18 also states that the security plan should fully identify and describe the controls currently in place, or planned for the system. However, Carson Associates found several areas in the Final System Security Plan for ADAMS, dated June 7, 2002, where controls were not described.

In order to identify what controls are currently in place for ADAMS, Carson Associates reviewed and analyzed two other documents in conjunction with the ADAMS Security Plan – the ADAMS self-assessment, and results from security test and evaluation of ADAMS controls conducted during the certification and accreditation of ADAMS.

FISMA requires agencies to test the management, operational, and technical controls of every information system identified in their inventory no less than annually. OMB has instructed agencies to use NIST SP 800-26, *Self-Assessment Guide for Information Technology Systems,* to conduct the annual reviews. NIST SP 800-26 is based on the Chief Information Officer Council's "Federal Information Technology Security Assessment Framework" (the Framework). The Framework comprises five levels to guide agency assessments of their security programs and assist in prioritizing efforts for improvement. Level 1 reflects that an asset has documented security policy. At Level 2, the asset also has documented procedures and controls to implement the policy. For Level 3, procedures and controls have been implemented to protect the asset. Level 4 indicates that procedures and controls are tested and reviewed. Finally, at Level 5, the asset has procedures and controls fully integrated into a comprehensive program.

Carson Associates reviewed the FY 2003 ADAMS self-assessment in order to identify controls in place for ADAMS. Any controls marked at least at a Level 3 in the ADAMS self-assessment are considered to be in place based on the above definitions. The FY 2003 self-assessment was reviewed as the agency had only provided a draft of the FY 2004 self-assessment when the fieldwork was conducted.

Carson Associates also reviewed the results of the security test and evaluation of ADAMS controls conducted during the certification and accreditation of ADAMS. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Appendix D of the ADAMS Security Test and Evaluation Plan and Report, dated June 14, 2002, includes test procedure worksheets used to record the results of the testing. The test objectives on the test procedure worksheets correspond to the control objectives in the NIST SP 800-26 self-assessment. Each test objective is marked as either pass, fail, or not applicable. A test objective marked as pass represents a security control that is in place.

As a result of the review of the ADAMS Security Plan, self-assessment, and security test and evaluation results, Carson Associates identified several cases where either the self-assessment and/or the test procedure worksheet indicated a control was in place, but it was not described in the Security Plan. The following are some examples:

- The ADAMS Security Plan does not describe the process for requesting, establishing, issuing, and closing user accounts. However, this control is marked as “pass” on the test procedure worksheets, and is marked as a Level 5 in the ADAMS self-assessment.
- The ADAMS Security Plan does not describe the processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media. This control is also marked as “pass” on the test procedure worksheets, and is marked as a Level 5 in the ADAMS self-assessment.
- The ADAMS Security Plan does not describe how lists of authorized users and their access are maintained and approved, if digital signatures are used, and whether access scripts with embedded passwords are prohibited. However, each of these controls is marked as a Level 5 in the ADAMS self-assessment, and is marked as “pass” on the test procedure worksheets.

Carson Associates also identified several instances where the information in the ADAMS Security Plan, self-assessment and test procedure worksheets is inconsistent. The following are some examples:

- The hardware and software maintenance controls related to reviewing a system to identify, and when possible, eliminate unnecessary services, and to periodically reviewing a system for known vulnerabilities and promptly installing software patches are marked as “fail” on the test procedure worksheets, but are marked as a Level 5 in the ADAMS self-assessment. These controls are not described in the ADAMS Security Plan.
- ***OFFICIAL USE ONLY PARAGRAPH REDACTED***
- The test control worksheets indicate that penetration testing is performed on the system. The ADAMS self-assessment indicates that extensive penetration testing is performed on the NRC local area network/wide area network that includes ADAMS at least every two years. The penetration testing is performed by OCIO. However, penetration testing is not described in the ADAMS Security Plan.
- Of the nine controls related to audit trails, seven are marked as “fail”, one as “pass,” and one as “not applicable” on the test procedure worksheets. The test procedure worksheets include a notation that ADAMS does not have the capability to audit user actions. However, all but two of the controls related to audit trails are marked as a Level 5 on the ADAMS self-assessment.

Finally, procedures for ensuring that users who no longer require access to ADAMS are removed from the system are described in the logical access controls section of the ADAMS Security Plan, which is contrary to guidance from NIST SP 800-18 and NIST 800-26. This control is found in the identification and authentication section of both NIST documents.

According to the agency, the ADAMS Security Plan is being updated in September 2004.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Executive Director for Operations:

2. Update the ADAMS Security Plan to describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

3. Update the ADAMS self-assessment to reflect controls in place. In-place controls are those that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

ADAMS Business Continuity Plan Is Not Consistent With NIST Guidelines

Carson Associates reviewed the ADAMS Business Continuity Plan (BCP), dated June 14, 2002, and a draft revised version dated May 20, 2004. Guidance on developing contingency plans can be found in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, which was published in June 2002. As recommended by OMB, Carson Associates reviewed the ADAMS BCP for consistency with NIST guidelines and found that in some instances, the ADAMS BCP is not consistent with NIST guidelines.

According to the agency, NRC requires annual updates of all BCPs, however NRC only requires conformance with current NIST guidance at the time of re-accreditation. This policy is not documented in any agency management directive or in any documentation reviewed by Carson Associates. Carson Associates was informed of this policy during the exit conference held to discuss the findings of the ADAMS system evaluation.

Subsequent to the exit conference, Carson Associates reviewed previous NIST guidance on the preparation of contingency plans, Federal Information Processing Standards (FIPS) Publication 87, *Guidelines for ADP Contingency Planning*, and found that the ADAMS BCP (both the 2002 and 2004 versions) is also not consistent with the FIPS 87 guidance. As stated earlier in this report, while the version of MD 12.5 that was in effect at the time the ADAMS BCP was first published did not require compliance with NIST guidelines, OMB requires agencies to follow NIST standards and guidance.

NIST SP 800-34 describes notification procedures and states that they should be documented in the plan for both events that occur with and without prior notice. For example, advanced notice is often given that a hurricane will affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. The procedures should describe the methods used to notify recovery personnel during business and non-business hours. Prompt notification is important for reducing the effects on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

NIST SP 800-34 also states that personnel to be notified in the event of a disaster should be clearly identified in the contact list appended to the plan. The list should identify personnel by their team position, name, and contact information (e.g., home number, work number, pager number, email address, and home address). FIPS 87 also stresses the importance of including the name, address, and phone numbers of all people who may be required in any backup or recovery scenario in the BCP.

However, some of the personnel contact information in the ADAMS BCP is not up to date and does not include notification procedures or contact information for notifying personnel during non-business hours. In some cases, the ADAMS BCP does not include personnel contact information for team leaders, alternate team leaders, or team members. For example, the BCP does not identify contact information for the team leader or alternate team leader for the Damage Assessment/Salvage Team, or contact information for the Disaster Recovery Coordinator and alternate during non-business hours. Not having up-to-date contact information to reach the designated teams during both business and non-business hours may cause delays in the disaster recovery process.

NIST SP 800-34 defines the reconstitution phase as when recovery activities are terminated and normal operations are transferred back to the organization’s facility. The reconstitution phase should specify teams responsible for restoring or replacing both the site and the system. The ADAMS BCP does not include procedures for restoring system operations that include procedures for cleaning the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. While FIPS 87 does not discuss specific procedures to be followed for cleaning the alternate site of any equipment or other materials belonging to the organization, these procedures are necessary to ensure that no sensitive materials remain at the alternate site.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

4. Update the ADAMS Business Continuity Plan to include the following changes:

    - Describe the methods used to notify recovery personnel during business and non-business hours for all scenarios.
    - Incorporate all teams roles and responsibilities and relevant points of contact information for team leaders, alternate team leaders, and team members for all scenarios.
    - Include procedures for restoring system operations, with a focus on how to clean the alternate site of any equipment or other materials belonging to the organization.

3.2 Security Protection Requirements Are Inconsistent Within Security Documentation

FISMA defines the term “information security” to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability is ensuring timely and reliable access to and use of information. Confidentiality, integrity and availability are often referred to as security protection requirements or security objectives for a system.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires all Federal agencies to categorize their systems by assigning potential impact levels to the three security objectives. The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.[12] The potential impact is moderate (medium) if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

The ADAMS Security Plan and the FY 2003 ADAMS self-assessment define protection requirements for ADAMS as follows:

- Confidentiality – High
- Integrity – High
- Availability – Medium

However, the FY 2004 ADAMS draft self-assessment defines protection requirements for ADAMS as follows:

- Confidentiality – High
- Integrity – High
- Availability – High

The protection requirements should be consistent across the security documentation for a system. A change in protection requirements could indicate a need to re-evaluate the risks to the systems, especially if the change is from a lower rating to a higher one. If the protection

[12] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

requirements have changed since the ADAMS Security Plan was finalized, then an explanation for the change should be noted on the ADAMS self-assessment.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

5. Update the ADAMS Security Plan and/or ADAMS self-assessment to consistently define the protection requirements (confidentiality, integrity, availability).

3.3 Findings and Recommendations Resulting From Testing Are Not Consistently Being Tracked

The FY 2003 FISMA independent evaluation of NRC's information security program found that the agency's corrective action process needed improvement. NRC has two primary tools for tracking the progress of corrective actions related to correcting weaknesses identified during the annual agency security review, the OIG independent evaluation, various security documents, and other security studies conducted by or on behalf of the agency. At a high level, NRC uses the plan of action and milestones (POA&M) submitted to OMB to track corrective actions from the OIG annual independent evaluation, and the agency's annual review. At a more detailed, level, NRC uses the NRC Information Technology Systems Security Tracking System (ITSSTS) to track the progress of internal corrective actions (i.e., those not reported to OMB). ITSSTS is used to track more specific corrective actions, such as those resulting from risk assessments; security test and evaluation associated with the certification and accreditation process; and contingency plan testing.

The FY 2003 FISMA independent evaluation of NRC's information security program also found that not all corrective actions resulting from security reviews and testing were being tracked. The OIG recommended that the agency identify all weaknesses and recommendations from security documentation and any other security reviews, and determine in which tool the recommendations will be tracked. In November 2003, OCIO issued a memo describing the agency's information technology security action item tracking process, strategy, and tools. The memo describes the types of activities that might identify security weaknesses in NRC information technology systems and describes the two tools used by NRC for tracking the process of security corrective actions – the FISMA POA&M and the ITSSTS. Carson Associates found that findings and recommendations resulting from testing of ADAMS security controls and from ADAMS contingency plan testing are not consistently being tracked.

Findings Resulting from the ADAMS Certification and Accreditation Are Not Consistently Being Tracked

The ADAMS Risk Assessment identified thirteen risks, and the Security Test and Evaluation Plan and Report identified eight risks. A Mitigation Plan submitted with the ADAMS certification and accreditation package in July 2002 combined the risks identified during the risk assessment and security test and evaluation into one list. Carson Associates could not account for four of the risks in the ADAMS Mitigation Plan in the current instance of ITSSTS. These risks were 1) ADAMS servers contain a multitude of questionable open ports and services, 2) the draft contingency plan is outdated and has never been implemented, tested, or approved by management, and no hot site[13] was identified, 3) incident response procedures have not been documented, and 4) ADAMS servers do not have anti-virus software installed.

According to the agency, these four risks were tracked and completed in 2002. At the exit conference held to discuss the findings of the ADAMS system evaluation, the agency provided documentation supporting their statement that the risks were tracked and completed in 2002 (output from a previous instance of the ITSSTS), but only for three of the four risks listed above. The agency could not determine why the three risks were not in the current instance of the ITSSTS and could not explain why the fourth risk could not be found in any instance of the ITSSTS.

Corrective Actions Resulting from the ADAMS BCP Testing Are Not Being Tracked

Carson Associates reviewed an OCIO memorandum dated March 15, 2004, regarding the successful completion of the ADAMS main library disaster recovery test. The memo states that on November 20, 2003, the ADAMS main library disaster recovery process was successfully tested and included restoration at the ADAMS off-site recovery facility. The testing resulted in five action items, however none of them are being tracked in the ITSSTS or in the agency's POA&M submitted to OMB.

RECOMMENDATION

The Office of the Inspector General recommends that the Executive Director for Operations:

6. Track all actions items resulting from testing of the ADAMS security controls and contingency plan in either the agency's internal tracking system or in the agency's plan of action and milestones submitted to OMB.

[13] A hot site is a fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster.

[Page intentionally left blank]

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Executive Director for Operations:

1. Update the ADAMS Risk Assessment Report to be consistent with National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide*.

2. Update the ADAMS Security Plan to describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

3. Update the ADAMS self-assessment to reflect controls in place. In-place controls are those that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

4. Update the ADAMS Business Continuity Plan to include the following changes:

   - Describe the methods used to notify recovery personnel during business and non-business hours for all scenarios.
   - Incorporate all teams roles and responsibilities and relevant points of contact information for team leaders, alternate team leaders, and team members for all scenarios.
   - Include procedures for restoring system operations, with a focus on how to clean the alternate site of any equipment or other materials belonging to the organization.

5. Update the ADAMS Security Plan and/or ADAMS self-assessment to consistently define the protection requirements (confidentiality, integrity, availability).

6. Track all actions items resulting from testing of the ADAMS security controls and contingency plan in either the agency's internal tracking system or in the agency's plan of action and milestones submitted to OMB.

5 OIG Response to Agency Comments

On September 15, 2004, the Executive Director for Operations provided comments concerning the draft system evaluation report. We modified the report as we determined appropriate in response to these comments.

SCOPE AND METHODOLOGY

To perform the ADAMS system evaluation, Carson Associates reviewed the system's security documentation, including the Security Plan, Risk Assessment, self-assessment, Business Continuity Plan, System Test and Evaluation Plan and Report, Certification and Accreditation documentation, and the completion of weaknesses addressed, if any, within the FY 2003 plan of action and milestones. Comprehensive document checklists were used in the evaluation process.

The work was conducted from June 2004 to August 2004 in accordance with guidelines from the National Institute of Standards and Technology, and best practices for evaluating security controls. Diane Reilly and Jane Laroussi from Carson Associates conducted the work.

[Page intentionally left blank]