OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION
DEFENSE NUCLEAR FACILITIES SAFETY BOARD

Evaluation of NRC's Agencywide Documents Access and Management System (ADAMS) Functional and Operational Capabilities

OIG-16-A-06
November 30, 2015

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

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

OFFICE OF THE
INSPECTOR GENERAL

November 30, 2015

MEMORANDUM TO: Victor M. McCree
Executive Director for Operations

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

SUBJECT: EVALUATION OF NRC'S AGENCYWIDE DOCUMENTS ACCESS AND MANAGEMENT SYSTEM (ADAMS) FUNCTIONAL AND OPERATIONAL CAPABILITIES (OIG-16-A-06)

Attached is the Office of the Inspector General's (OIG) evaluation report titled *Evaluation of NRC's Agencywide Documents Access and Management System (ADAMS) Functional and Operational Capabilities*.

The report presents the results of the subject evaluation. Following the November 16, 2015, exit conference, agency staff indicated that they had no formal comments for inclusion in this report.

Please provide information on actions taken or planned on each of the recommendations within 30 days of the date of this memorandum. Actions taken or planned are subject to OIG followup as stated in Management Directive 6.1.

We appreciate the cooperation extended to us by members of your staff during the evaluation. If you have any questions or comments about our report, please contact me at (301) 415-5915 or Ziad Buhaissi, Contracting Officer's Representative (COR), at (301) 415-1983.

Attachment: As stated

Office of the Inspector General

U.S. Nuclear Regulatory Commission
Defense Nuclear Facilities Safety Board

OIG-16-A-06

November 30, 2015

Results in Brief

Why We Did This Review

The Agencywide Documents Access and Management System (ADAMS) is the Nuclear Regulatory Commission's (NRC) repository for Official Agency Records. It has been in place since November 1999 and has to meet NRC's document management needs while also complying with Federal mandates for electronic recordkeeping and public access requirements. The Office of Information Services manages ADAMS staff in headquarters and regional offices use ADAMS for their day-to-day mission activities. The public uses NRC's public site to access Web-Based ADAMS.

The Office of the Inspector General (OIG) contracted AEGIS.net, Inc., to evaluate if ADAMS meets its required operational capabilities and adequately provides for functionality such as serving as the agency's repository for Official Agency Records, searching, usability, document storage and retrieval, and other aspects such as availability, performance, contingency planning, and security.

The evaluation objective was to determine if ADAMS meets its required operational capabilities and adequately provides for functionality.

Evaluation of NRC's Agencywide Documents Access and Management System (ADAMS) Functional and Operational Capabilities

What We Found

The evaluation team examined ADAMS' functionality and operational capabilities in each of three areas: Federal and NRC Guidance, User Requirements, and Information Technology (IT) System Requirements. Based on this work, the evaluation team found that ADAMS has the capability to serve as the agency's repository for official agency records. However, opportunities exist to improve ADAMS' Federal and NRC records management, search and retrieval functionality, and management oversight over ADAMS operation.

A summary of the evaluation findings is as follows:

1. **Federal and NRC Guidance:** ADAMS does not currently satisfy records disposition objectives.

2. **User Requirements:** ADAMS search and retrieval functionality occasionally returns irrelevant or incomplete results.

3. **ADAMS IT System Requirements**:
   A. ADAMS is operating without a current Authority to Operate (ATO).
   B. ADAMS has not fully implemented National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 4.
   C. Management of ADAMS system configurations and security documentation is not consistently implemented.
   D. Many ADAMS planned security remediation activities are delayed.

What We Recommend

This report makes recommendations to implement ADAMS' Records Manager module, to improve ADAMS' search and retrieval functionality, and to insure compliance with security standards and configuration management best practices. A consolidated list of recommendations for addressing the findings is included in section IV of this report. Agency management stated their general agreement with the report.

TABLE OF CONTENTS

ABBREVIATIONS AND ACRONYMS..... i

I. BACKGROUND 1
II. OBJECTIVE 2
III. FINDINGS 2

A. ADAMS Does Not Currently Satisfy Records Disposition Objectives 3
Recommendations 5
B. ADAMS Search and Retrieval Functionality Occasionally Returns Irrelevant or Incomplete Results 5
Recommendations 7
C. ADAMS IT Requirements Related Findings 8
a. ADAMS Is Operating without A Current Authority to Operate 9
Recommendations 11
b. ADAMS Has Not Fully Implemented NIST SP 800-53 Rev 4 11
Recommendations 14
c. Management of ADAMS System Configurations and Security Documentation Is Not Consistently Managed 14
Recommendations 18
d. Many ADAMS Planned Security Remediation Activities Are Delayed 19
Recommendations 21

IV. CONSOLIDATED LIST OF RECOMMENDATIONS 22
V. AGENCY COMMENTS 24

APPENDIXES

A. OBJECTIVE, SCOPE, AND METHODOLOGY 25
B. REFERENCES 29

TO REPORT FRAUD, WASTE, OR ABUSE 37

COMMENTS AND SUGGESTIONS 37

ABBREVIATIONS AND ACRONYMS

Term	Description
ADAMS	Agencywide Documents Access and Management System
ADAMS-P8	ADAMS Panagon 8
ADAMS RM	ADAMS Record Manager
ATO	Authority to Operate
CFR	Code of Federal Regulations
CM	Configuration Management
CRDS	NRC Comprehensive Records Disposition Schedule
CSO	Computer Security Office
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
ISSO	Information System Security Officer
IT	Information Technology
IT/IM	Information Technology/Information Management
MD	Management Directive
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OARs	Official Agency Records
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget

POA&Ms	Plan of Action and Milestones
Rev	Revision
RM	Records Management
RMF	Risk Management Framework
RPS	Reactor Program System
SP	Special Publication
SSP	System Security Plan
Super user	Office designated person with primary responsibility for input of documents into ADAMS
VAR	Vulnerability Assessment Report
WBA	Web-Based ADAMS

I. BACKGROUND

ADAMS is NRC's repository for Official Agency Records (OARs). It has been in place since November 1999 and has to meet NRC's document management needs while also complying with Federal mandates for electronic recordkeeping and public access requirements. The Office of Information Services (OIS) manages ADAMS and staff in headquarters and regional offices use it for their day-to-day mission activities. The public uses NRC's public site to access Web-Based ADAMS. ADAMS Original was upgraded to a new version of IBM Filenet Platform, called Panagon 8 (ADAMS P8), in December 2010.

Accomplishment of NRC's core mission is of the utmost importance and management of the documentation of these efforts is critical to the core mission as it provides the evidence of NRC actions to inform future efforts, to report to the Government, and to communicate to the public. As NRC's repository for OARs, ADAMS has to comply with Federal guidelines as well as internal NRC Management Directives (MD). Not only has guidance increased over time, but the definition of official agency records has grown with development of new technologies, to include e-mails and their attachments, Blackberry and wireless, Instant Messaging and other social media (e.g., wikis and blogs), permanent scanned images, digital photographic records, Portable Document Format records, digital geospatial data records, web content records, and additional formats such as digital and video, that must be addressed. As ADAMS scope broadens and evolves to encompass these new content and IT system requirements, simultaneously, it continues to be tailored to satisfy the user communities it serves - NRC staff, NRC management, and the public.

Although the emphasis of this evaluation is on areas for improvement so that ADAMS continues to meet its mission for the agency, we do note that ADAMS and the records management infrastructure have been recognized with the following awards:

- the Archivist of the United States Award of Excellence in 2004, and
- Workflow Management Coalition Global Awards for Excellence in

Case Management 2015 winner for Excellence in Case Management, June 23, 2015

The NRC Office of the Inspector General (OIG) retained AEGIS.net, Inc. to perform this evaluation of ADAMS. This report presents the results of the evaluation.

II. OBJECTIVE

The objective of this evaluation was to perform an independent evaluation of NRC's ADAMS to determine if it meets its required operational capabilities and adequately provides the necessary functionality to serve as the agency's repository for OARs. This includes providing functionality such as document storage, document search and retrieval, ease-of-use (i.e., usability), and other aspects such as availability, performance, contingency planning, and security. This evaluation also includes a review of relevant NRC policies and procedures that define what and how documents are input, how and who can access them, and for how long they are stored since ADAMS efficacy is directly affected by these policies and procedures.

III. FINDINGS

The findings of this evaluation consider that it is not only the system components and capabilities that determine ADAMS effectiveness and efficiency in meeting its functional requirements, but that agency policies and processes determine what is entered into the system, the quality of those records, and that the associated metadata strongly impact whether ADAMS can meet its primary obligation as the NRC repository for OARs.

A. ADAMS Does Not Currently Satisfy Records Disposition Objectives

As NRC's repository for OARs, ADAMS has to comply with Federal guidelines, such as those published by the National Archives and Records Administration (NARA), as well as internal NRC MD. Federal Guidelines include the Presidential Directive on Managing Government Records[1] issued by NARA, and Office of Management and Budget (OMB). Other Federal requirements such as the Open Government Initiative, Code of Federal Regulations (CFR) specifically 36 CFR, chapter 12, subchapter B and C, and the IT accessibility requirements defined in Rehabilitation Act Section 508 govern additional capabilities that ADAMS must provide.

What Is Required

The records disposition objectives described in NRC's MD 3.53, *NRC Records and Document Management Program*, states the following: "Preserve records of continuing value" and "Destroy records of temporary value as soon as they have served their purpose." MD 3.53 also states the following: "NARA regulations require NRC to maintain and preserve permanent records and to ensure that temporary records are promptly disposed of or retired when no longer needed."

In addition, the CFR Title 36 chapter XII, subchapter B, Part 1224.10, d states: "Incorporate records retention and disposition functionality during the design, development, and implementation of new or revised recordkeeping systems (whether paper or electronic)." Subpart C, Part 1236.20 provides additional requirements for electronic recordkeeping functionality, to include: "(7) *Execute disposition.* Identify and effect the transfer of permanent records to NARA based on approved records schedules. Identify and delete temporary records that are eligible for disposal. Apply records hold or freeze on disposition when required."

[1] Presidential Memorandum – Managing Government Records, November 28, 2011.

What We Found

Currently, ADAMS does not transfer permanent records or destroy temporary records as per NUREG – 0910, NRC's Comprehensive Records Disposition Schedule (initial version published July 1982). The initial ADAMS Original and the upgrade ADAMS P8 (FY 2010), were both implemented without the capability to manage this aspect of a record's lifecycle. As per interviewee comments, the initial records management software, 'Foremost', only allowed users to manually file documentation within ADAMS Original and did not allow for disposition implementation. This was replaced by the IBM Enterprise Records software called ADAMS Record Manager (RM). However ADAMS RM has yet to be configured and implemented fully. As per NARA, final disposition of records is a basic record management function.[2] Therefore, ADAMS, without a fully functioning RM tool does not manage a record throughout its entire lifecycle.

Why This Occurred

ADAMS RM can be used to manage records retention schedules. However, it was not configured and installed during the implementation of ADAMS P8.

Why This Is Important

If ADAMS cannot manage the complete lifecycle of a record, NRC may fall behind schedule in implementation of its RM duties and risk non-compliance with NARA guidelines. This could also impact ADAMS

[2] National Archives' NARA Electronic Records Management (ERM) policy documents and guidance http://www.archives.gov/records-mgmt/policy/prod6b.html

operational and functional capabilities to ensure transparency, efficiency, and accountability as the agency's electronic recordkeeping system.

Recommendations

OIG recommends that the Executive Director for Operations

1. Expedite and fully implement the ADAMS RM module so that records retention schedules can be attached to all the official records within ADAMS.

B. ADAMS Search and Retrieval Functionality Occasionally Returns Irrelevant or Incomplete Results

In the area of user requirements, we reviewed how well ADAMS supports user needs including ease of use, search and retrieval functions, personal (dashboard and reporting) customization, and in general, how well it meets user defined needs. Survey respondents were generally satisfied with ease of use. Search and retrieval issues, however, were reported by users and found to be related to variations in the document input processing and profiling across the agency offices and among individual users.

What Is Required

The CFR (specifically 36 CFR, chapter XII, subchapter B, Part 1236), states: "*As part of the capital planning and systems development life cycle processes, agencies must ensure:… b) That all records in the system will be retrievable and usable for as long as needed to conduct agency business … ."* Further, 36 CFR chapter XII, subpart C, Part 1236.20 includes 7 requirements, among them particular points addressing access and retrieval: "(5) *Manage access and retrieval.* Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records." And "(6) *Preserve records.* Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet NARA-approved dispositions. Agencies must develop procedures to enable the migration of records and their

associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence." Search and retrieval functionality is one of the most important aspects of a document repository. Users need to be confident that their findings are complete and accurate. This is especially true in the cases of record searches when responding to a Freedom of Information Act (FOIA) request, discovery, or in support of the internal activities that support NRC's mission.

What We Found

The evaluation team found that ADAMS users are generally dissatisfied with the search and retrieval functionality. ADAMS presents the user with a variety of search options including search templates, custom search options, and the new Enterprise Search tool. However, ADAMS users are unclear about which search options would be optimal under various usage scenarios.

Users stated that search results contained what they considered to be irrelevant documents and incomplete sets of documents. One super user[3] reported, "The search function outside of the standard search templates is of little help, and is often not accurate. I can perform a search using accurate criteria for a document and it will return erroneous results and will often times leave documents that meet these criteria out of the results."

Interviewees also mentioned that approximately 600-800 templates exist to support profiling.[4] These templates were created in response to individual user/NRC office requests. The new Enterprise Search function is implemented. However, the users were largely unaware of this tool.

[3] Office designated person with primary responsibility for input of documents into ADAMS.
[4] There are a total of 226 final templates in ADAMS.

Why This Occurred

Issues exist with the use and population of ADAMS profiles and templates which affects search effectiveness. The profiling process that feeds into the ADAMS search functionality is not uniformly used across offices. A survey responder said, "Not all offices require their staff to profile documents in accordance with an ADAMS template making it difficult to search for documents." ADAMS has an inordinately large number of templates to support profiling and processing requirements.

Information is not entered into ADAMS consistently. There is inconsistent use of ADAMS between offices and between individual users, resulting in variations for documents that are stored in ADAMS and how they are coded for retrieval (profiling, key words, etc.). Some individuals upload a PDF image of a document instead of a PDF document that recognizes the actual text inside the document.

Why This Is Important

Information retrieved may not be complete for NRC to effectively report on its mission activities to the government and public; and to conduct them in the first place when access to historical information is needed.

Recommendations

OIG recommends that the Executive Director for Operations

2. Fully implement the new Enterprise Search tool to help address the existing issues regarding search and retrieval.

3. Reduce the number of templates and study applicability of automation techniques to pre-fill profile metadata and attain better standardization and consistency.

4. Place hyperlinks directly in ADAMS to quick reference guides, how-to guidance, RM training, and other ADAMS training, to remind users about the ADAMS features and RM responsibilities.

C. ADAMS IT Requirements Related Findings

The evaluation team reviewed IT aspects of ADAMS related to performance, availability, configuration management, and security. ADAMS security documentation was reviewed for compliance with NIST standards and guidelines, and the NRC CSO Risk Management Program and related cyber risk management activities that must be implemented at the agency and system levels. When the evaluation was being conducted, ADAMS has an overall security categorization of High. Many of the recommended controls were already in place, and there was a Plan of Action and Milestones (POA&Ms) for the planned controls.

We found that ADAMS performance and availability was not an issue. However, system shortfalls were noted in compliance with security standards and adherence to configuration management best practices, specifically:

1. ADAMS is operating without a current Authority to Operate (ATO)
2. ADAMS has not fully implemented NIST SP800-53 Rev 4
3. Management of ADAMS system configurations and security documentation is not consistently managed
4. Many ADAMS planned security remediation activities are delayed

The recently appointed ADAMS Information System Security Officer is expected to advance compliance in the above-mentioned areas.

a. ADAMS Is Operating Without a Current Authority to Operate

What Is Required

The NIST Special Publication (SP) 800-37, "Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems" describes a methodology that incorporates Federal Information Security Management Act security standards and guidance to provide a solution for managing risk to an organization's information and information systems. According to Step 5 (Authorize) of the NIST RMF, SP 800-57 provides guidelines that describe the steps leading to system authorization within the Risk Management Framework:

- Ensure authorizing officials are appropriately engaged throughout the risk management process
- Promote a better understanding of organizational risks resulting from the operation and use of information systems
- Support consistent, informed security authorizations decisions

Furthermore, Step 6 (Monitor) of the NIST RMF guides agencies to implement an effective continuous monitoring program which includes security status reporting to appropriate organizational officials and active involvement by authorizing officials in the ongoing management of information system-related security risks.

Additionally, Federal Information Processing Standards Publications (FIPS) 200 specifies minimum security requirements for information and information systems supporting the federal agencies. For high-impact information systems, organizations must, at a minimum, employ appropriately tailored security controls from the high baseline of security controls defined in NIST SP 800-53 and must ensure that the minimum assurance requirements are satisfied.

NRC Computer Security Office (CSO) Standards and Guidance[5]

NRC's CSO-PROS-1323, "Information Security Continuous Monitoring Process" defines the process that must be followed to perform continuous monitoring on systems owned and used by NRC. Also the NRC CSO-PROS-1323 (Section 3.4.1) process and NRC Office Instruction CSO-STD-0020, Organization Defined Values for System Security Controls, (Section 3.4.4) standard requires system owners to update the security authorization at least every three years or upon major system modification for high sensitivity information systems.

What We Found

According to the ADAMS ATO Memo,[6] the ADAMS ATO expired on January 20th, 2014. The test result for security control CA-6.1.2 'Determine if the authorizing official authorizes the information system for processing before commencing operations' in the ADAMS Authorization System Cybersecurity Assessment Report[7] states - *"ADAMS received its Authorization to Operate (ATO) on January 20, 2011 (ML103560073). In addition, ADAMS received an ATO extension until 9/30/2015."*
No risk related to the ADAMS expired ATO was captured in the Security Assessment Report and no related weakness was captured as an actionable item in the POA&Ms. ADAMS is operating without a current ATO or any documented risk acceptances from the Designated Approving Authority.

Subsequent to the end-of-fieldwork, an NRC official told us that ADAMS has been issued a verbal ATO and is operating under a current ATO as of 09/29/2015. However, no formal ATO memorandum has been issued.

[5] As of November 1, 2015, the Computer Security Office became the Information Security Directorate.
[6] ADAMS Authority to Operate Memo, January 20, 2011, ML103560073
[7] ADAMS Authorization System Cybersecurity Assessment Report ML15201A705

Why This Occurred

The current Information System Security Officer was appointed this past year inheriting the ADAMS ATO expiration issue. Management stated that resource constraints also delayed creation of a new ATO package.

Why This Is Important

An ATO is evidence that the Designated Approving Authority has been provided with an in-depth understanding of the security posture and risks of a system and has made a risk-informed decision to allow that system to enter operation at NRC. Without it the Designated Approving Authority does not have updated, recent information about ADAMS security posture and risks needed for them to make an informed decision about whether continued ADAMS operation should be authorized.

Recommendations

OIG recommends that the Executive Director for Operations

5. Obtain the needed ATO.

b. ADAMS Has Not Fully Implemented NIST SP 800-53 Rev 4

What Is Required

FIPS 200 requires that any approved changes to NIST SP 800-53 must be employed by federal agencies within one year from the date of final publication. NIST SP 800-53, Revision 4 (April 2013), represents the most comprehensive update to the security controls catalog since its inception in 2005. NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, includes several changes

from SP 800-53 Rev. 3. There were 295 controls and control enhancements added while approximately 100 controls and control enhancements were withdrawn or incorporated into others. Of the 18 security control families in SP 800-53 Rev. 4, 17 families are described in the Security Control Catalog (NIST SP 800-53 Appendix F), and are closely aligned with the 17 minimum security requirements for federal information and information systems in FIPS 200.

NRC CSO Standards and Guidance

The FY 2015 Cybersecurity Risk Management Activities Instructions memorandum[8] issued by the Office of the Executive Director for Operations requires system owners to take the following actions:

- Update system security documentation, (particularly the System Security Plan (SSP), Security Risk Assessment, POA&Ms, Security Categorization Report, and the Privacy Threshold Analysis/Privacy Impact Assessment, etc.) to ensure that the system security posture is accurately documented as changes are made, and/or as threats, vulnerabilities, technologies, and business requirements and processes evolve.

- Update any supporting documentation (e.g., configuration management plan, documented configurations in recovery, rebuild, or other operational support procedures, inventory, system architecture document, and design document) to reflect changes to the system and/or organization within 60 calendar days of change and placed in ADAMS (upon request) for CSO and/or OIG review. Changes must be tracked and approved as part of a formal change control process.

This memorandum document also includes a reference to NIST SP 800-53 Rev. 4 for any additional guidance.

[8] FY 2015 Cybersecurity Risk Management Activities Instructions memorandum, January 15, 2015

What We Found

ADAMS has not fully implemented NIST SP 800-53 Revision 4, "Assessing Security and Privacy Controls in Federal Information System and Organizations" security controls. As of September 30, 2015 ADAMS does have an updated SSP that includes SP 800-53 Rev 4 security controls, which they plan on submitting during their next security quarterly update as part of their continuous monitoring process. According to NIST compliance standards, federal agencies have up to one year from the date of final publication (April 2013) to fully comply with the changes but are encouraged to initiate compliance activities immediately.

Subsequent to end-of-fieldwork, the ADAMS Information System Security Officer provided a link to an updated version of the SSP that includes SP800-53 Rev 4 security controls. While a final SSP including Rev 4 has not yet been officially submitted, this evidence does indicate that updating the SSP to the latest revision has been initiated.

Why This Occurred

ADAMS continued to implement corrective measures to address deficiencies in the SP 800-53 Rev 3 security controls and to reduce or eliminate known vulnerabilities, and was not fully prepared to implement the SP 800-53 Rev 4 by the April 2014 due date. CSO guidance regarding Rev 4 implementation was delayed as NRC worked on deciding on the NRC-specific "org-defined values."

Why This Is Important

ADAMS may be vulnerable to risks posed by evolving technology and threat space (characterized by the increasing sophistication of cyber-attacks and the operations tempo of adversaries) that are addressed by additional guidance for security controls and control enhancement in the

NIST SP 800-53 Rev 4. The SP 800-53 Rev 4 controls provide organizations with additional security controls necessary to strengthen the resilience of their information systems in the face of cyber-attacks and other threats.

Recommendations

OIG recommends that the Executive Director for Operations

6. Upgrade ADAMS security posture to meet NIST SP 800-53, Rev 4.

c. Management of ADAMS System Configurations and Security Documentation Is Not Consistently Managed

What Is Required

NIST SP 800-53 Rev 3 describes a disciplined and structured process that integrates configuration management activities into the system development lifecycle. NIST SP 800-53 guides organizations to:

- Develop configuration management procedures
- Establish, document, and maintain required baseline configurations settings for IT components (software, hardware, server, etc.) of an information system
- Monitor and control changes to configuration items and settings; analyze changes to the information system to determine potential security impacts prior to change implementation
- Develop, document and maintain an inventory of information system components to accurately reflect the current information system
- Scan for vulnerabilities in the information system; analyze vulnerability scan reports and results, and remediate appropriate vulnerabilities in accordance with an organization assessment of risk

NRC CSO Standards and Guidance

NRC CSO has developed system configuration standards and processes to be used in the protection of any information system that stores, transmits/receives, or processes NRC information.

Step 4 of the NRC CSO Risk Management Framework requires vulnerability scans and configuration checks of system components. In addition, according to the FY 2015 Cybersecurity Risk Management Activities Instructions memorandum, NRC CSO-STD-0020 standard (NRC Office Instruction CSO-STD-0020, Organization Defined Values for System Security Controls) and NRC CSO- PROS-1401 process, the system owners should scan, patch, and check the configuration compliance of their systems with the rigor and frequency based on the system sensitivity level. Furthermore, the NRC CSO-STD-0020 standard also states that critical vulnerabilities should be remedied within 21 calendar days and high vulnerabilities within 45 calendar days.

What We Found

During FY15 scanning and testing of ADAMS, multiple findings were discovered related to ADAMS server and applications configurations not meeting NRC standards and guidelines. Based on the test results of the vulnerability scan conducted from May 7, 2015 through June 10th, 2015, assessors discovered 21 critical, 599 high, 46 moderate, and three low findings. A large number of high findings were related to system components not being configured in accordance with CSO standards. Most of these findings were present from previous scanning reports that have not been addressed.

According to ADAMS ATO POA&Ms (FY15 Q4 dated August 12, 2015), there are 67 open POA&M items related to Configuration Management (CM) controls.

The ATO package referenced in the ADAMS Authorization memorandum submitted by the ISSO to the Executive Director for Operations for review/approval on August 13, 2015 included draft versions of the following documents instead of approved versions –

- Draft version of Authorization System Cybersecurity Assessment Report, July 9th, 2015. Note: When this issue was brought up during this evaluation, the ISSO provided the latest up-to-date version of the ADAMS Authorization System Cybersecurity Assessment Report (Rev 1.0, dated July 27th, 2015) to the evaluation team.
- Draft version of ADAMS Vulnerability Assessment Report (VAR) FY 15 Authorization System Cybersecurity Assessment, July 9th, 2015.[9]

The Senior Information Technology Officer did not officially approve ADAMS Security Categorization document[10], and the unapproved version was submitted as part of the ADAMS Authority to Operate package to the Executive Director for Operations.

An inconsistency was found between ADAMS SSP Rev 1.36, ADAMS Security Categorization and ADAMS Business Impact Assessment. The SSP document states that ADAMS consists of 26 core components, which are grouped into eight segments, whereas, the Security Categorization and Business Impact Assessment documents state that ADAMS consists of 24 core components which are grouped into eight segments.

ADAMS ATO SSP Rev 1.36 references Reactor Program System (RPS) Memorandum of Understanding[11] and Interconnection Security Agreement.[12] Neither document had the needed signatories.

[9] ADAMS Vulnerability Assessment Report (VAR) FY15 Authorization System Cybersecurity Assessment, ML15201A710
[10] ADAMS Security Categorization Report, ML15084A050
[11] Memorandum of Understanding Between OIS and NRR Regarding ADAMS-RPS Interconnection, 2013 ML13009A428
[12] Interconnection Security Agreement Between OIS and NRR Regarding ADAMS-RPS Interconnection, 2013 ML13025A147

The ADAMS ATO System Security Plan Rev 1.36 dated July 27, 2015, is not reflective of the current status of the controls within the system. Subsequent to end-of-fieldwork, ADAMS team indicated that they are working on a get well plan to address the scanning results for the Designated Approving Authority.

Why This Occurred

While NRC has defined baseline configuration management standards for its systems and applications, the ADAMS implementation processes to ensure compliance with these baselines have not matured. Most of the findings from previous scanning and assessment reports have not been addressed and the ADAMS support team continues to have issues remediating weaknesses in a timely manner.

There was a lack of adherence to NRC CSO applicable standards, procedures, or process descriptions. While packaging artifacts for the ADAMS ATO, the Information System Security Officer or the contractor personnel inadvertently picked up the draft versions of the Authorization System Cyber Security Assessment and VAR reports from the Draft Document Class folder. During the last quarterly update of the ADAMS SSP, the security team inadvertently missed updating the status of security controls relating to six POA&M items.

Why This Is Important

The configuration management and configuration control processes are an essential element of an effective security control monitoring program. The integrity and correctness of the security artifacts is important to establish and maintain security of the information system. Failure to receive an approval from the NRC Senior IT Security Officer may hinder ADAMS re-authorization process.

The SSP is used to maintain an accurate status of the security posture of the information system, and to support risk management activities at the

management level. Not having an updated SSP provides management with an inaccurate picture of ADAMS security status which may lead to ineffective system risk management.

Recommendations

OIG recommends that the Executive Director for Operations

7. Implement NRC Information Security Directorate and NIST procedures for the consistent implementation of configuration management controls in ADAMS.

8. Configure ADAMS servers, applications, and other IT components according to NRC Information Security Directorate standards and requirements.

9. Apply corrective actions to eliminate vulnerability threats or mitigate identified risks and communicate those actions to NRC senior management as appropriate.

10. Implement quality assurance/peer review practices to ensure that the final version of the artifact follows the applicable NRC Information Security Directorate procedures and is accurate and consistent with other documents.

11. Obtain Senior IT Security Officer approval on ADAMS Security Categorization document.

12. Update the ADAMS SSP to reflect the current status of POA&Ms.

d. Many ADAMS Planned Security Remediation Activities Are Delayed

What Is Required

FISMA and OMB require Federal agencies to develop, maintain, and monitor POA&Ms. The plan of action and milestones is a key document in the information security program and is subject to Federal reporting requirements established by OMB. POA&Ms are documents that are used to identify, assess, prioritize and monitor the progress of corrective actions for security weaknesses found in overall security program and information systems. NIST SP 800-53 Rev 3 security control CA-5 (POA&M) and PM-4 (POA&M process) guides Federal agencies to develop and implement a plan of action and milestones for the information system to document the organization's planned remedial action to correct deficiencies or weaknesses found during the assessment of security control, and to eliminate or reduce known vulnerabilities in the system. POA&Ms should be updated based on the finding from security impact analysis, security control assessment, and continuous monitoring activities.

Step 6 of NIST SP 800-37 Risk Management Framework requires agencies to perform remediation of outstanding items listed in the POA&Ms on an ongoing basis. In accordance with OMB policy, the agencies are required to assess a subset of the security controls annually during continuous monitoring.

NRC CSO Standards and Guidance

NRC CSO-PROC-2104 and CSO-PROC-2016 describe processes for NRC to identify, assess, prioritize, and monitor the progress of corrective actions relating to security weaknesses and provides agency direction for the management and tracking of corrective efforts relative to known weaknesses in the IT security controls. Listed below are a few specific requirements described in the CSO-PROC-2104 and CSO-PROC-2016 related to NRC POA&Ms:

- To support quarterly OMB reporting requirements, POA&Ms should be updated within the automated tool by the system owner with the most current information by the 15 of November, February, May, and August.

- According to NRC CSO-PROC-2104, a POA&M is found deficient if 4 or more of the open POA&M items have completion due dates that are more than 1 year old; or greater than 25 percent of the open POA&M items have completion due dates that are more than 1 year old.

What We Found

At the time of evaluation, we found that 74 POA&Ms are in the delayed status. Out of 74 delayed POA&M items, 51 are categorized as High requiring immediate or near-immediate corrective action and 23 are categorized as Moderate.

Why This Occurred

Resource constraints affect the amount of dedicated time spent on POA&M resolution. Addressing POA&Ms requires several groups including, the ADAMS team, data center contractors, development contractors, and security contractors; each group has its own priorities and there is no overall owner in charge of all the groups.

Why This Is Important

POA&Ms are a management tool used to track and monitor the progress of corrective actions relative to known weaknesses in security controls. Not addressing POA&Ms in a timely manner prolongs the time that NRC is exposed to the risk represented by the POA&M.

Recommendations

OIG recommends that the Executive Director for Operations

13. Remediate security weaknesses in ADAMS and escalate priority conflicts to respective NRC senior managers as needed to improve timely resolution of delayed POA&Ms.

IV. CONSOLIDATED LIST OF RECOMMENDATIONS

OIG recommends that the Executive Director for Operations

Federal and NRC Guidance

1. Expedite and fully implement the ADAMS RM module so that records retention schedules can be attached to all the official records within ADAMS.

User Requirements – Search and Retrieval

2. Fully implement the new Enterprise Search tool to help address the existing issues regarding search and retrieval.

3. Reduce the number of templates and study applicability of automation techniques to pre-fill profile metadata and attain better standardization and consistency.

4. Place hyperlinks directly in ADAMS to quick reference guides, how-to guidance, RM training, and other ADAMS training, to remind users about the ADAMS features and RM responsibilities.

IT System Requirements

5. Obtain the needed ATO.

6. Upgrade ADAMS security posture to meet NIST SP 800-53, Rev 4.

7. Implement NRC Information Security Directorate and NIST procedures for the consistent implementation of configuration management controls in ADAMS.

8. Configure ADAMS servers, applications, and other IT components

according to NRC Information Security Directorate standards and requirements.

9. Apply corrective actions to eliminate vulnerability threats or mitigate identified risks and communicate those actions to NRC senior management as appropriate.

10. Implement quality assurance/peer review practices to ensure that the final version of the artifact follows the applicable NRC Information Security Directorate procedures and is accurate and consistent with other documents.

11. Obtain Senior IT Security Officer approval on ADAMS Security Categorization document.

12. Update the ADAMS SSP to reflect the current status of POA&Ms.

13. Remediate security weaknesses in ADAMS and escalate priority conflicts to respective NRC senior managers as needed to improve timely resolution of delayed POA&Ms.

V. AGENCY COMMENTS

A discussion draft of this report was provided to the agency prior to an exit conference held on November 16, 2015. Agency management provided comments that have been incorporated into this report, as appropriate. As a result, management stated their general agreement with the report and will not provide formal comments.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this evaluation was to perform an independent evaluation of NRC's ADAMS to determine if it meets its required operational capabilities and adequately provides the necessary functionality to serve as the agency's repository for OARs. This includes providing functionality such as document storage, document search and retrieval, ease-of-use (i.e., usability), and other aspects such as availability, performance, contingency planning, and security.

Scope

We conducted this evaluation at NRC headquarters (Rockville, MD) from July 2015 through November 2015. Internal controls related to the evaluation objective were reviewed and analyzed. Throughout the evaluation, evaluators were aware of the possibility of fraud, waste, or abuse in the program.

Methodology

For the purpose of this evaluation, the various attributes of the ADAMS system to be reviewed were grouped into three broad areas of investigation. We looked at how ADAMS:

1. provides operational capabilities and functionality as the agency's repository for OARs;
2. satisfies user needs for searching, usability, and document storage and retrieval needs;
3. provides appropriate IT availability, performance, configuration management, contingency planning and how it has met security requirements.

The focus of the assessment was the "as-is" state of ADAMS at the point in time in which the assessment was performed, and so the evaluation was conducted on the current ADAMS P8. ADAMS consists of multiple libraries, and this evaluation focused on the main library and Web-Based ADAMS. The evaluation team utilized the process depicted below in Figure 1 to examine the current capabilities of ADAMS and develop recommendations and applicability of best practices.

Figure 1 - Analysis Methodology

Our methodology consisted of several specific assessment activities:

- Observation – direct inspection of the use and behavior of the system.
- Examination of Documentation – review of documented requirements, technical and end user documentation, industry, federal and agency-specific standards and guidelines, to develop a clear understanding of the system and what it was designed to do. We also researched relevant best practices and leading methodologies.
- Hands-on Testing – direct use to provide further insight into the operation of the system as well as verification/validation of the correct implementation of requirements. The evaluation team tested ADAMS functionality and observed ADAMS walkthroughs and use by an NRC system administrator and a super user. All available iLearn ADAMS training classes were reviewed, and the ADAMS intranet site was examined in detail.
- Corroborative Inquiry – additional verification/validation was conducted through interviews with stakeholders including program leaders, business users, and development/integration contractors. The team conducted in-person and telephone interviews and a survey of NRC users representing the Office of Information Services, Office of the Advisory Committee on Reactor Safeguards (ACRS), the Office of Administration (ADM), the Office of Nuclear Material Safety and Safeguards (NMSS), the Office of New Reactors (NRO), the Office of

Nuclear Reactor Regulation (NRR), the Office of Enforcement (OE), and the NRC Regional Offices III and IV.

Note that individual comments, findings and observations may not be reflective of the whole organization but are individual data points collected, observed or discussed in interviews during this evaluation. Additionally, leading methodologies, standards and industry best practices were evaluated for applicability to the ADAMS operations and maintenance activities. We reviewed ADAMS capability and functionality across a range of attributes. These were organized into three broad areas of review as summarized in the table below.

Specific Attributes as Identified	Federal/NRC Repository Requirements	User Requirements	IT System Considerations
Ability and efficacy as repository for NRC's Official Agency Records.	✓		
Ability to appropriately process, store and display publicly and non-publicly available documents	✓		
Search functionality		✓	
Document storage and organization	✓	✓	
Personalization and ease of use		✓	
Reporting functionality		✓	
Contingency plans			✓
System performance			✓
System Security and Risk Management			✓
Compliance with applicable Federal mandates (e.g., Section 508)	✓		✓
Systems requirements documentation, latest work flow diagrams and other process or business diagrams for accuracy and implementation in the system.	✓		
System configuration and design documentation for accuracy and implementation in the system. Additional system documentation included, but was not limited to, system interface requirements, user training materials, data migration plans, contingency plans and security documentation.		✓	✓
Application of applicable industry standards, federal standards, and best practices.	✓	✓	✓

Table 1 - Attributes Reviewed by Area

The evaluation was conducted by the following staff from AEGIS.net, Inc.: Tom Lourenco (Evaluation Manager), Agi Seaton, Suman Subhash, and Ruth Briscoe.

Appendix B

REFERENCES (documentation/information reviewed)

ADAMS 508 Exception Memo, DRAFT, July 2010

ADAMS Authority to Operate Memo January 20, 2011, ML103560073

ADAMS Authorization System Cybersecurity Assessment Report, ML15201A705

ADAMS_Authorization_System_Cybersecurity_Assessment_Report_v1.0_20150727 (Revised for ATO)

ADAMS Business Impact Analysis Rev 1.4, ML14318A404

ADAMS Configuration Management Plan Revision 1.4, ML110750615

ADAMS Contingency Test Report v1.0, ML15167A483

ADAMS Desk Reference Guide, August 2008, ML051110390

ADAMS Deviation Request for ADAMS ATO, ML15224B468

ADAMS Document Input Simplification Business Process Improvement, Management Presentation, August 2015

ADAMS Document Submission Guidelines – Step-by-Step Instructions, August 6, 2009

ADAMS-EIE Interconnection Security Agreement 2012_ML12209A267

ADAMS-EIE Memorandum of Understanding 2012_ML12209A266

ADAMS Functional Test.pdf, ML15044A199

ADAMS FY15 ASCA VAR FTS, Ml15201A712

ADAMS FY15 Q4 ASCA POA&Ms, ML15209A907 (as of August 12th, 2015)

ADAMS ISSO Appointment Letter, ML14143A163

ADAMS P8 Report Error Message.pdf, ML15049A106

ADAMS P8 Requirements, Open ADAMS P8 Folder (1 – Requirements)

ADAMS P8 Workplace XT User Manual v2.2.1 October 1, 2013, ML110831112

ADAMS Response to Formal Deviation Request, ML12132A338

ADAMS Revised Privacy Impact Assessment, February 23, 2015, ML15055A041

ADAMS Security Categorization Report, ML15084A050

ADAMS Security Risk Assessment Rev 1.0, ML15209A946

ADAMS System Cybersecurity Assessment Plan Rev 1.0, ML15201A700

ADAMS System Security Plan (SSP) Rev 1.36, July 2015, ML103220552

ADAMS User Group Meeting Notes 10/30/2013
http://pbadupws.nrc.gov/docs/ML1334/ML13345A039.pdf

ADAMS User Group Meeting Notes 11/5/14
http://pbadupws.nrc.gov/docs/ML1434/ML14349A562.pdf

ADAMS User Group Meeting Notes 4/29/15
http://pbadupws.nrc.gov/docs/ML1515/ML15155B269.pdf

ADAMS User Group Meeting Notes 5/14/14
http://pbadupws.nrc.gov/docs/ML1418/ML14181B248.pdf

ADAMS User Group Meeting Notes 5/8/13
http://pbadupws.nrc.gov/docs/ML1315/ML13154A027.pdf

ADAMS User Training Tutorial Videos
http://www.internal.nrc.gov/ois/ECM/ADAMS/index.html

ADAMS Vulnerability Assessment Report (VAR) FY15 Authorization System Cybersecurity Assessment, ML15201A710

Agency Use of the FileNet Platform v1.1. April 2015, ML15177A267

AIIM ARP1-2009 – Analysis, Selection, and Implementation of Electronic Document Management Systems (EDMS)
http://www.aiim.org/documents/standards/ARP1-2009.pdf

American National Standards Institute - ANSI/PMI 99-001-2008

American National Standards Institute (ANSI) Framework for Integration of Electronic Document Management Systems and Electronic Records Management Systems (ANSI/AIIM TR48-2004) http://www.ansi.org

ANSI/IEEE Standard 1012-2004 Software Verification and Validation

ARMA International, Generally Accepted Recordkeeping Principles (GARP),
http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles

ATO Recommendation Memo SUNSI CSO-ADM-5001

Audit and Accountability Policy and Procedures Office of Information Services (OIS) Agencywide Documents Access and Management System (ADAMS) ML13301A505

Authority to Discontinue Tracking Low Cybersecurity Risks as Plan of Action and Milestone Items, ML15089A208

Blog ADAMS User Group http://www.nrc.gov/reading-rm/adams/users-group.html

Business Analysis for Practitioners: A Practice Guide, Project Management Institute, January, 2015

CMMI for Development (CMMI-DEV), v1.3, November, 2010

Common Questions About Federal Records and Related Agency Requirements http://www.fas.org/sgp/crs/secrecy/R43072.pdf

Contingency Plans ML15120A168

Corrective Actions NARA Audit

Digitization Plan ML12209A268

DoD 5015.2 – Electronic Records Management Software Applications Design Criteria Standard http://jitc.fhu.disa.mil/recmgt/standards.html

DOE – Records Management Responsibilities 2010 http://energy.gov/sites/prod/files/cioprod/documents/Your_Records_Management_Responsibilities2_.pdf

Executive Order 13556 Controlled Unclassified Information, https://www.whitehouse.gov/the-press-office/2010/11/04/executive-order-13556-controlled-unclassified-information

File Types That Can Be Declared as Official Agency Records http://www.internal.nrc.gov/ois/divisions/irsd/adams/pdf/ML061740176.pdf

FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems

GAO-12-331G, Government Auditing Standards: 2011 Revision (Supersedes GAO-07-731G) [Reissued on January 20, 2012]

Government Paperwork Elimination Act (GPEA) Public Law 105-277, Title XVII

Implement Enterprisewide Records Management to Meet Your Compliance Requirements, Gartner, January 21, 2015.

Information and Records Management Program, Electronic Signatures Project Plan V1.0 June 19, 2015

Information and Records Management Program – Plans and Activities, Fiscal Years 2014-2019. OIS, IT/IM Portfolio Management and Planning Division, IT/IM Policy Branch, October 17, 2014. ML13295A575

Institute of Electrical and Electronics Engineers IEEE STANDARD 1490-2011 - IEEE Guide--Adoption of the Project Management Institute (PMI(R)) Standard A Guide to the Project Management Body of Knowledge (PMBOK(R) Guide)--Fourth Edition

Interconnection Security Agreement Between OIS and NRR Regarding ADAMS-RPS Interconnection, 2013 ML13025A147

ISO 9001:2008 Quality management systems – Requirements http://www.iso.org/iso/catalogue_detail?csnumber=46486

ISO 15489 1 & 2 – Information and Documentation – Records Management

ISO 23081 – 2:2009 – Information and Documentation – Managing Metadata for Records

Memorandum of Understanding Between OIS and NRR Regarding ADAMS-RPS Interconnection, 2013 ML13009A428

NARA Final Rule, Electronic Mail Systems, and General Records Schedule (GRS) 20, Disposition of Electronic Records

NARA Managing Government Records Directive – Automated Electronic Records Management Report/Plan, September 19, 2014

NARA Records Management Oversight Inspection Report 2014, United States Nuclear Regulatory Commission Records Management Program

NARA Bulletin 2010-02 - Continuing Agency Responsibilities for Scheduling Electronic Records http://www.archives.gov/records-mgmt/bulletins/2010/2010-02.html

National Archives' NARA Electronic Records Management (ERM) Guidance on the Web http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html (although this page is superseded by Transfer Guidance for various records formats, other areas of applicability include:

National Archives' NARA Electronic Records Management (ERM) policy documents and guidance

- Examples of System Functions for Electronic Recordkeeping (ERK) and Electronic Records Management (ERM) http://www.archives.gov/records-mgmt/policy/prod6b.html
- Records Management (RM) Profile in the Federal Enterprise Architecture (FEA); ERM E-Gov Initiative - Recommended Practice: Analysis of Lessons Learned for Enterprise-wide ERM Projects, Guidance for Building an Effective Enterprise-wide Electronic

  Records Management (ERM) Governance Structure, Electronic Records Management Guidance on Methodology for Determining Agency-unique Requirements; Electronic Record Keeping (ERK) checklists and activities; managing web records; PKI-unique administrative records; electronic signature; etc. located under: http://www.archives.gov/records-mgmt/policy
- For emerging web technologies including instant messaging, digital audio and video records, Optical Storage Media, sustainable formats; located under: http://www.archives.gov/records-mgmt/initiatives
- NARA records management training available nationwide. http://www.archives.gov/records-mgmt/training/training.html
- Vital Records and Records Disaster Mitigation and Recovery - http://www.archives.gov/records-mgmt/vital-records/recovery.html

National Checklist Program Repository
https://web.nvd.nist.gov/view/ncp/repository

NIST SP 800-18, Guide for Developing Security Plans for Information Technology Systems and Organizations

NIST SP 800-34, Contingency Planning Guide for Federal Information Systems

NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems

NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

NIST SP 800-53 Rev 3, Recommended Security Controls for Federal Information Systems

NIST SP 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organization

NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems

NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

NRC ADAMS MOMCE Service Level Agreement ML12206A498

NRC ADAMS Website contents

NRC Announcement - December 19, 2008 - Policy Reminder: Reminder that NRC Employees and Contractors Must Comply with the Recordkeeping Requirements http://www.internal.nrc.gov/announcements/items/4890.html

NRC Authority to Use Process CSO-PROS-1325

NRC CSO Cybersecurity Risk Management Activities Instructions Fiscal Year 2015
http://www.internal.nrc.gov/CSO/documents/FY2015%20Cybersecurity%20Risk%20Management%20Activities%20Memo.pdf
NRC CSO Plan of Action and Milestones Process CSO-PROS-2016

NRC CSO System Artifact Examination Procedure CSO-PROC-2104

NRC's Information Technology/Information Management (IT/IM) Strategic Plan for Fiscal years (FYs) 2015-2019

NRC Enterprise Content Management Program, Records Management Readiness and Current State Review DRAFT Version 1.0, January 11, 2010

NRC Management Directive 2.8 – Project Management Methodology

NRC Management Directive 3.53 – NRC Records and Document Management Program Rev. 4

NRC Management Directive 12.5 – NRC Cybersecurity Program

NRC NUREG-0910: NRC Comprehensive Records Disposition Schedule, July 1982

NRC NUREG-0910: NRC Comprehensive Records Disposition Schedule, Rev. 4, March 2005

NRC OIG: Audit of NRC's Freedom of Information Act Process, OIG-14-A-17, ML# 14181B048

NRC OIG: Audit of NRC's Information Technology Governance, OIG-14-A04, ML# 13343A244

NRC OIS Organizational Chart from NRC Intranet

NRC Records Management Assessment Project Deliverable 1: Records Management Program Assessment Report, January 19, 2010

NRC Risk Management Framework Process CSO-PROS-2030

NRC Web-Based iLearn training reviewed: ADAMS P9 – Overview Course ID_1361, ADAMS P8 –Basic - Course ID_1281, ADAMS P8 – Advanced – Course ID_1301, NRC Records Management Training – Course ID_151144

OMB Memorandum M-11-29: Chief Information Officer Authorities, August 8, 2011

OMB Memorandum M-12-18: Managing Government Records Directive, August 24, 2012 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf

Open Government National Action Plan for the United States of America, 2011 and 2013 http://www.archives.gov/open/

POA&MS Review Checklist v1.9.2, ML100840319

Presidential and Federal Records Act Amendments of 2014

Presidential Memorandum – Managing Government Records, November 28, 2011 https://www.whitehouse.gov/the-press-office/2011/11/28/presidential-memorandum-managing-government-records

Project Management Body of Knowledge Guide, Fifth Edition, Project Management Institute, released in 2013

Section 508 of the Rehabilitation Act.

Service Level Agreement between ICOD and IRSD for ADAMS, ML11138A228

Title 10 of the Code of Federal Regulations (CFR), Part 9, Public Records

Title 36 of the Code of Federal Regulations (CFR), Chapter 12 Subchapter B, Records Management. (NARA Regulations)

Title 36 of the Code of Federal Regulations (CFR), Chapter 12 Subchapter B, Part 1236- Electronic Records Management http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=36:3.0.10.2.25

Title 41 of the Code of Federal Regulations (CFR), 201-9 General Services Administration (GSA) regulations

U.S. Nuclear Regulatory Commission Agency-wide Continuous Monitoring Program CSO-PROS-1323

U.S. Nuclear Regulatory Commission's (NRC) Information Technology/Information Management (IT/IM) Strategic Plan for Fiscal Years 2016 – 2020, ML14316A302

Yellow Announcement 2000-039 Revised Policy Goal on Timing the Release of Documents to the Public in the ADAMS Environment, May 22, 2000 http://www.internal.nrc.gov/announcements/yellow/2002-1997/2000-039.html

TO REPORT FRAUD, WASTE, OR ABUSE

Please Contact:

Email: Online Form

Telephone: 1-800-233-3497

TDD 1-800-270-2787

Address: U.S. Nuclear Regulatory Commission
Office of the Inspector General
Hotline Program
Mail Stop O5-E13
11555 Rockville Pike
Rockville, MD 20852

COMMENTS AND SUGGESTIONS

If you wish to provide comments on this report, please email OIG using this link.

In addition, if you have suggestions for future OIG audits, please provide them using this link.