EVALUATION REPORT

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2007

OIG-07-A-19 September 28, 2007

September 28, 2007

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL YEAR 2007 (OIG-07-19)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2007.*

This report presents the results of the subject audit. Agency comments provided at the exit conference on September 17, 2007, have been incorporated, as appropriate, into this report. The agency provided formal comments, which appear in Appendix E of the report. Appendix F contains the detailed OIG analysis of agency comments.

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 follow up as stated in Management Directive 6.1. Note that the recommendations made in the Fiscal Year 2005 and Fiscal Year 2006 FISMA evaluations, which are resolved but still require agency action in order to be closed, will now be tracked under this year's FISMA report.

We appreciate the cooperation extended to us by members of your staff during the audit. If you have any questions or comments about our report, please contact me at 415-5915, or Beth Serepca, Team Leader, Security and Information Management Team, at 415-5911.

Attachment: As stated

Electronic Distribution

Frank P. Gillespie, Executive Director, Advisory Committee on Reactor
  Safeguards/Advisory Committee on Nuclear Waste
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and
  Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
William M. McCabe, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
William F. Kane, Deputy Executive Director for Reactor
  and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research,
  State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Information Services
  and Chief Information Officer, OEDO
Vonna L. Ordaz, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
  and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
R. William Borchardt, Director, Office of New Reactors
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
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

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2007

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

September 25, 2007

The views, opinions, and findings contained in this report are those of the authors and should not be construed as an official 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, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine its effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. FISMA requires the annual evaluation to be performed by the agency's Inspector General (IG) or by an independent external auditor.

Office of Management and Budget (OMB) memorandum M-07-19, *FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 25, 2007, requires the agency's IG to complete the OMB FISMA Reporting Template for IGs (referred to by OMB as Section C). That template, along with any additional narrative the IG believes would provide meaningful insight into the status of the agency's security or privacy program, is submitted to OMB as part of the agency's annual FISMA report, and is included as Appendix D to this report.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on August 17, 2007. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible.

PURPOSE

The objective of this review was to perform an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for FY 2007.

RESULTS IN BRIEF

Program Enhancements and Improvements

To correct weaknesses identified by the FY 2005 and FY 2006 FISMA independent evaluations by the NRC Office of the Inspector General (OIG), and to address findings from the agency's own evaluations, the agency has refocused its information system security program. Under the refocused program, the agency proposed performing certification and accreditation of systems that are a high priority from a mission perspective and others that potentially pose a higher security risk (e.g., agency systems that communicate with systems outside the NRC network). The first certification and accreditation schedule under the refocused program was issued in February 2006. This schedule has changed several times since February 2006.

[1] For the purposes of FISMA, the agency uses the term "information system security program."

The agency has accomplished the following since the FY 2006 FISMA independent evaluation:

- The agency developed a new certification and accreditation process. The agency has finalized the templates for all certification and accreditation documents as well as instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology.
- As required by FISMA, NRC performed annual testing and evaluation (also referred to as self-assessment) of the security controls for 28 of the agency's 30 operational systems. As the other two agency operational systems were just certified and accredited in FY 2007, the agency did not perform an additional self-assessment of those systems as permitted by OMB and National Institute of Standards and Technology (NIST) guidance.
- The agency updated security plans for 5 of the agency's 30 operational systems. Subsequent to the completion of fieldwork, the agency provided an updated security plan for another system.
- The agency completed the consolidation and reconciliation of data from NRC information systems inventory systems and created a new centralized system for tracking NRC information systems.
- The agency has developed policies, procedures, and a template for conducting privacy impact assessments (PIA).
- The agency has made significant progress in implementing the provisions of OMB memorandum M-06-15, *Safeguarding Personally Identifiable Information*, as well as subsequent memoranda issued by OMB regarding privacy and the protection of personally identifiable information (PII).

Significant Deficiencies

The following significant deficiencies were identified in NRC's information system security program. These significant deficiencies were also identified in the FY 2006 FISMA independent evaluation, and were reported as findings in the FY 2005 FISMA independent evaluation.

- Only 2 of the 30 operational NRC information systems have a current certification and accreditation, and only 4 of the 11 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation. Subsequent to the completion of fieldwork, the agency completed certification and accreditation of one of the contractor systems for which they have direct oversight, and the system was granted an authorization to operate (ATO). Two additional agency systems have also been certified and are currently under review by the agency's designated approving authority for consideration of an ATO.
- Annual contingency plan testing is still not being performed for all systems.

Program Weaknesses

The independent evaluation also identified 12 information system security program weaknesses. Five are repeat findings from the FY 2005 and FY 2006 FISMA independent evaluations and are identified in the body of the report. The following seven findings are new.

- Security categorizations for some systems do not consistently reflect the information types that reside on the systems.
- The agency did not follow OMB and NIST guidance when conducting its annual self-assessments.
- Self-assessments were not always based on approved security categorizations.
- Self-assessments contained errors and inconsistencies.
- The agency's methodology is flawed for identifying which listed systems reside on the NRC network and which do not.
- The quality of the agency's plans of action and milestones (POA&Ms) needs improvement.
- The agency's certification and accreditation process is inconsistent with NIST guidance.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA. A consolidated list of recommendations appears on page 45 of this report.

AGENCY COMMENTS

At an exit conference with the agency held on September 17, 2007, the agency provided informal written comments and generally agreed with the report recommendations. The NRC Chief Information Officer provided a formal response to this report on September 24, 2007. Appendix E contains the Chief Information Officer's transmittal letter. The agency's formal comments along with OIG's analysis and response to those comments are included as Appendix F. This final report incorporates revisions made, where appropriate, in response to the agency's comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Document Access and Management System
ATO	Authorization to Operate
BPIAD	Business Process Improvement and Applications Division
Carson Associates	Richard S. Carson and Associates, Inc.
CIO	Chief Information Officer
COOP	Network Continuity of Operations
DISA	Defense Information Systems Agency
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IATO	Interim Authorization to Operate
IG	Inspector General
IRSD	Information and Records Services Division
ISS	Information System Security
IT	Information Technology
LAN/WAN	Local Area Network/Wide Area Network
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
POA&M	Plan of Action and Milestones
SP	Special Publication
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team

[Page intentionally left blank]

TABLE OF CONTENTS

Appendices

List of Tables

1 Background

On December 17, 2002, the President signed the E-Government Act of 2002, which included FISMA.[2] FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine its effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. FISMA requires the annual evaluation to be performed by the agency's IG or by an independent external auditor.

OMB memorandum M-07-19 requires the agency's IG to complete the OMB FISMA Reporting Template for IGs. That template, along with any additional narrative the IG believes would provide meaningful insight into the status of the agency's security or privacy program, is submitted to OMB as part of the agency's annual FISMA report.

Richard S. Carson and Associates, Inc. (Carson Associates), performed an independent evaluation of NRC's implementation of FISMA for FY 2007. This report presents the results of that independent evaluation. Carson Associates also prepared the OMB FISMA Reporting Template for IGs, along with additional narrative, for inclusion in the agency's annual FISMA report. The OMB FISMA Reporting Template for IGs and the additional narrative is included as Appendix D to this report.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on August 17, 2007. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible.

2 Purpose

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2007. Appendix A contains a description of the evaluation scope and methodology.

3 Findings

Over the past 5 years, NRC has made improvements to its information system security program, and continues to make progress in implementing the recommendations resulting from previous FISMA evaluations. To correct weaknesses identified by the FY 2005 and FY 2006 FISMA independent evaluations by the OIG, and to address findings from the agency's own evaluations, the agency has refocused its information system security program. Under the refocused program, the agency proposed performing certification and accreditation of systems that are a high priority from a mission perspective and others that potentially pose a higher security risk (e.g., agency systems that communicate with systems outside the NRC network). The first

[2] 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.

certification and accreditation schedule under the refocused program was issued in February 2006. This schedule has changed several times since February 2006.

The security certification and accreditation of information systems is integral to an agency's information security program and is an important activity that supports the risk management process required by FISMA. Section 3.7 of this report provides an in-depth discussion of the certification and accreditation process and its significance to an agency's information security program.

The first phase of the refocused program also included the development of a new certification and accreditation process, which has been finalized. The agency has finalized the templates for all certification and accreditation documents as well as instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology.

The agency has also accomplished the following since the FY 2006 FISMA independent evaluation:

- As required by FISMA, NRC performed annual testing and evaluation (also referred to as self-assessment) of the security controls for 28 of the agency's 30 operational systems. As the other two agency operational systems were just certified and accredited in FY 2007, the agency did not perform an additional self-assessment of those systems as permitted by OMB and NIST guidance.
- The agency updated security plans for 5 of the agency's 30 operational systems. Subsequent to the completion of fieldwork, the agency provided an updated security plan for another system.
- The agency completed the consolidation and reconciliation of data from NRC information systems inventory systems and created a new centralized system for tracking NRC information systems.
- The agency has developed policies, procedures, and a template for conducting PIAs.
- The agency has made significant progress in implementing the provisions of OMB memorandum M-06-15, as well as subsequent memoranda issued by OMB regarding privacy and the protection of PII.

However, even with the new certification and accreditation process, the refocused information system security program, and the award of a multi-year, multi-million dollar contract to provide the agency with consolidated information system security services, the agency has completed certification and accreditation of only two agency systems and one contractor system for which the agency has direct oversight in the past 2 years. In the meantime, the certifications and accreditations for all of the agency's remaining 28 operational systems have expired.

The following significant deficiencies were identified in NRC's information system security program. These significant deficiencies were also identified in the FY 2006 FISMA independent evaluation, and were reported as findings in the FY 2005 FISMA independent evaluation.

- Only 2 of the 30 operational NRC information systems have a current certification and accreditation, and only 4 of the 11 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation. Subsequent to the completion of fieldwork, the agency completed certification and accreditation of one of the contractor systems for which they have direct oversight, and the system was granted an ATO. Two additional agency systems have also been certified and are currently under review by the agency's designated approving authority for consideration of an ATO.
- Annual contingency plan testing is still not being performed for all systems.

The independent evaluation also identified 12 information system security program weaknesses. Five are repeat findings from the FY 2005 and FY 2006 FISMA independent evaluations, and seven are new.

- Security categorizations for some systems do not consistently reflect the information types that reside on the systems (new finding).
- The majority of NRC major applications and general support systems have not been categorized in accordance with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (repeat finding).
- The agency did not follow OMB and NIST guidance when conducting its annual self-assessments (new finding).
- Self-assessments were not always based on approved security categorizations (new finding).
- Self-assessments contained errors and inconsistencies (new finding).
- The agency does not maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements (repeat finding).
- Oversight of other contractor systems is lacking (repeat finding).
- The agency's methodology is flawed for identifying which listed systems reside on the NRC network and which do not (new finding).
- The quality of the agency's POA&Ms needs improvement (new finding).
- The agency's certification and accreditation process is inconsistent with NIST guidance (new finding).
- The agency lacks procedures for ensuring employees with significant information technology (IT) security responsibilities receive security training (repeat finding).
- E-authentication risk assessments have not been completed (repeat finding).

The following sections present the detailed findings from the independent evaluation. As stated previously, two findings are significant deficiencies, seven findings are new, and five are repeat findings from previous FISMA independent evaluations. The following sections are organized based on the OMB FISMA Reporting Template for IGs, which can be found in Appendix D of this report. Each major section corresponds to a question or set of questions from the template. Findings are presented in the sections to which they are relevant.

3.1 FISMA Systems Inventory

<u>Agency Systems</u>

OMB Requirement	OIG Response
1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized) (a., b., and c.). *1.a. Agency Systems.*	*See Table 3-1 below.*

Table 3-1. Total Number of Agency Systems by FIPS 199 Risk Impact Level

FIPS 199 Risk Impact Level	Total Number	Number Reviewed
High	4	0
Moderate	11	1
Low	0	0
Not Categorized	15	0
Total	30	1

NRC has a total of 30[3] operational systems that fall under FISMA reporting requirements.[4] Of the 30, 17 are general support systems,[5] and 13 are major applications.[6] As required by FISMA, Carson Associates selected a subset of NRC systems for evaluation during the FY 2007 FISMA independent evaluation. However, only one of the three systems that were selected had a current certification and accreditation. While an additional system completed certification and accreditation in July 2007, it was after the cutoff date established at the entrance conference, and was therefore not considered for evaluation. As there were no other systems with a current certification and accreditation to consider for evaluation, Carson Associates evaluated only one agency system for the FY 2007 FISMA independent evaluation.

[3] The agency reports 31 operational systems. The OIG disagrees with the agency that an OIG system is a major application. It has been categorized as a listed system since it began operations in 2004. This designation is presently under a detailed review. Therefore, the metrics in this report reflect a total of 30 operational systems.

[4] NRC also has a number of major applications and general support systems currently in development. For FISMA reporting purposes, only operational systems are considered.

[5] A general support system is an interconnected set of information resources under the same direct management control that share common functionality. Typical general support systems are local and wide area networks, servers, and data processing centers.

[6] A major application is a computerized information system or application that requires special attention to security because of the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

A current certification and accreditation is needed to perform a system evaluation because it contains a description of the current security controls that are in place or are planned for a system. This information is found in the system's security plan, which is a part of a system's certification and accreditation package. An understanding of whether the security controls that are in place are operating as intended, as well as any risk associated with operating the system with the described security controls, is also necessary for performing a system evaluation. This information is also found in the system's certification and accreditation package.

Contractor Systems

OMB Requirement	OIG Response
1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized) (a., b., and c.). *1.b. Contractor Systems.*	*See Table 3-2 below.*

Table 3-2. Total Number of Contractor Systems by FIPS 199 Risk Impact Level

FIPS 199 Risk Impact Level	Total Number	Number Reviewed
High	0	0
Moderate	4	0
Low	1	0
Not Categorized	6	0
Total	11	0

NRC has a total of 11 systems operated by a contractor or other organization on behalf of the agency (8 major applications and 3 general support systems). Of the 11, 6 are operated by other Federal agencies, 2 are operated by federally funded research and development centers, and 3 are operated by private contractors. NRC is responsible for direct oversight for four of these systems. Oversight of the remaining seven systems is the responsibility of the Federal agency operating the system. Therefore, the OIGs of those agencies would be responsible for evaluating those systems.

As required by FISMA, Carson Associates selected a subset of the contractor systems for which NRC is responsible for direct oversight for evaluation during the FY 2007 FISMA independent evaluation. However, the system selected did not have a current certification and accreditation, and none of the other contractor systems for which NRC is responsible for direct oversight had a current certification and accreditation. Therefore, Carson Associates did not evaluate any contractor systems for the FY 2007 FISMA independent evaluation.

Security Categorization – Background

FIPS 199 requires all Federal agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The security categorization of an information system is conducted by first categorizing all information types[7] resident on the information system. The security category of an information type is established by determining the potential impact (i.e., low, moderate, high) for each security objective (i.e., confidentiality, integrity, availability) associated with the particular information type. For example, an organization managing public information on its Web server determines that there is no potential impact from a loss of confidentiality (i.e., confidentiality requirements are not applicable), a moderate potential impact from a loss of integrity, and a moderate potential impact from a loss of availability.

The security categorization of an information system must take into account the security categories of all information types resident on the information system being categorized. For an information system, the potential impact values assigned to the respective security objectives are the highest values (i.e., high water mark) from among the security categories that have been determined for each information type resident on the information system.

Since the potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system, the high water mark concept must be used to determine the overall impact level of the information system. Thus, a low-impact system is an information system in which all three of the security objectives are low. A moderate-impact system is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a high-impact system is an information system in which at least one security objective is high. Therefore, the information system used in the above example would be considered a moderate-impact system.

The determination of information system impact levels must be accomplished prior to the consideration of minimum security requirements and the selection of appropriate security controls for those information systems.

FINDING A – Security Categorizations for Some Systems Do Not Consistently Reflect the Information Types that Reside on the Systems (New Finding)

Carson Associates reviewed the security categorizations for 9 agency systems and 3 contractor systems and found that 4 do not consistently reflect the information types that reside on the systems. As a result, the overall impact levels of these information systems may not reflect the impact to the agency should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

[7] Information is categorized according to its information type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive order, directive, policy, or regulation.

The NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volume I, describes the following methodology for identifying information types when conducting a security categorization:

- Identify the fundamental business areas (management and support) or mission areas (mission-based) supported by the system under review.
- Identify for each business or mission area the areas of operations or lines of business that describe the purpose of the system in functional terms.
- Identify the sub-functions necessary to carry out each area of operation or line of business.
- Select the basic information types associated with the identified sub-functions.
- Where appropriate, identify any information type processed by the system that is required by statute, Executive order, or agency regulation to receive special handling.

To determine the primary information types that reside on the systems for which security categorizations were reviewed, Carson Associates reviewed the agency's Exhibit 53[8] for FY 2007. Carson Associates found that the security categorizations for four systems did not reflect the primary business area, primary line of business, and/or primary sub-function of those systems as indicated on the Exhibit 53. Table 3-3 below shows a comparison of the primary information type indicated on the Exhibit 53 with the information types found in the security categorizations for the four systems.

Table 3-3. Primary Information Type Comparison – Exhibit 53 and Security Categorization

System	Primary Information Type in Exhibit 53	Information Types in Security Categorization
System 1	Catastrophic Defense	Disaster Monitoring and Prediction, IT Security, Environmental Monitoring and Forecasting
System 2	Catastrophic Defense	Customer Services, Official Information Dissemination, IT Security, Record Retention, Information Management, Disaster Monitoring and Prediction, Disaster Preparedness and Planning, Environmental Monitoring and Forecasting
System 3	Information Management	Scientific and Technical Research and Innovation, Research and Development, IT Security
System 4	Corrective Action	Program Evaluation, Program Monitoring, Budget Formulation, Strategic Planning, Management Improvement, Official Information Dissemination, Inspections and Auditing, Standards Setting/Reporting Guideline Development

[8] The Exhibit 53 is used by agencies to report their IT investment portfolio annually to OMB. The Exhibit 53 provides budget estimates for all IT investments and identifies those that are major investments.

If the security categorizations do not reflect the information types that reside on the systems, the overall impact levels of these information systems may not reflect the impact to the agency should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

RECOMMENDATION

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

1. Review and correct as needed all security categorizations so that they consistently reflect the information types that reside on the systems.

FINDING B – Majority of NRC Major Applications and General Support Systems Have Not Been Categorized in Accordance With FIPS 199 (Repeat Finding)

This is a repeat finding from the FY 2005 and FY 2006 FISMA independent evaluations. As stated previously, FIPS 199 requires all Federal agencies to categorize their information systems. However, despite this requirement, the majority of NRC major applications and general support systems still have not been categorized in accordance with FIPS 199. Specifically, only 15 of the 30 operational NRC information systems have been categorized. Only 5 of the 11 contractor systems have been categorized.

In FY 2007, the agency completed only three additional security categorizations for NRC systems, updated the security categorization for another system, and completed four additional security categorizations for contractor systems. According to the agency, the target date for completing all system security categorizations was August 15, 2007. This target date was not met.

Without security categorizations for all agency and contractor systems, the agency cannot effectively determine minimum security requirements and select appropriate security controls for their information systems as defined in NIST SP 800-53 Revision 1, *Recommended Security Controls for Federal Information Systems*. In addition, the agency cannot be assured it is using the correct minimum security control baseline from NIST SP 800-53 when performing its annual security control testing and review. The security categorization is also needed to effectively implement several Federal and OMB initiatives.

RECOMMENDATION

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

2. Categorize all NRC major applications and general support systems in accordance with FIPS 199. This recommendation replaces recommendation #1 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

3.2 Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

3.2.1 Certification and Accreditation

OMB Requirement	OIG Response
2. For the total number of systems reviewed by component/bureau and FIPS system impact level for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy. *2.a. Number of systems certified and accredited.*	*See Table 3-3 below (NOTE: the metrics represent the status for all NRC systems, not just the subset that was chosen for evaluation in FY 2007).*

Table 3-3. Number of Systems Certified and Accredited by FIPS 199 Risk Impact Level

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	1	0	1
Moderate	1	4	5
Low	0	1	1
Not Categorized	0	0	0
Total	2	5	7

This section reports on the number of agency and contractor systems with a current certification and accreditation. Section 3.7 of this report discusses the assessment of the agency's certification and accreditation process in detail.

FINDING C – The Majority of NRC Systems Are Not Certified and Accredited (Repeat Significant Deficiency)

As in FY 2005 and FY 2006, Carson Associates found that the majority of NRC systems are not certified and accredited. Only 2 of the 30 operational NRC information systems have a current certification and accreditation. Of the 11 systems operated by a contractor or other organization on behalf of the agency, only 4 have a current certification and accreditation. These four systems are operated by other Federal agencies. Of the remaining seven, two are operated by other Federal agencies, two are operated by federally funded research and development centers, and three are operated by private contractors. Subsequent to the completion of fieldwork, the agency completed certification and accreditation of one of the contractor systems for which they have direct oversight, and the system was granted an ATO. Two additional agency systems have also been certified and are currently under review by the agency's designated approving authority for consideration of an ATO.

OMB defines a significant deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets." OMB Circular A-130, *Management of Federal Resources,* Appendix III, *Security of Federal Automated Information Resources*, provides three specific examples of a significant deficiency, each of which must be reported as such – (1) the failure to assign responsibility for security of the system or application, (2) the lack of a system security plan, and (3) the absence of authorization to process (certification and accreditation).

In accordance with OMB requirements, it constitutes a ***significant deficiency*** that only 2 of the 30 operational NRC information systems have a current certification and accreditation and only 5 of the 11 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation. This deficiency is not a recent problem. The agency has made little progress in correcting the deficiency. The agency has completed certification and accreditation of only two agency major applications and one contractor system for which the agency has direct oversight in the past 2 years. According to the agency, certification and accreditation of all agency systems is not expected to be completed until the end of FY 2009.

3.2.2 Security Control Test and Evaluation

OMB Requirement	OIG Response
2. For the total number of systems reviewed by component/bureau and FIPS system impact level for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy. *2.b. Number of systems for which security controls have been tested and reviewed in the past year.*	*See Table 3-4 below.*

Table 3-4. Number of Systems With Tested and Evaluated Security Controls by FIPS 199 Risk Impact Level

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	4	0	4
Moderate	11	2	13
Low	0	1	1
Not Categorized	15	3	18
Total	30	6	36

FISMA requires that the management, operational, and technical controls[9] in agency systems be tested with a frequency depending on risk, but not less than annually. NRC meets this requirement by performing annual self-assessments of the security controls of all agency and contractor systems. The purpose of the self-assessment is to assess the security controls in an information system 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.

NRC performed self-assessments of the security controls for 28 of the agency's 30 operational systems. The agency chose not to perform a self-assessment of the OIG system discussed earlier, as that system's status as a major application is still under determination. As the other two agency operational systems were just certified and accredited in FY 2007, the agency did not perform an additional self-assessment of those systems as permitted by OMB and NIST guidance. The agency also included the physical and environmental controls of the four NRC regional offices and the NRC Technical Training Center in one self-assessment.

NRC is required to perform self-assessments only on those contractor systems for which it has direct oversight. Self-assessments for the remaining contractor systems are the responsibility of the Federal agencies that operate those systems. NRC performed a self-assessment of one of the four contractor systems for which it has direct oversight. As two of the four contractor systems for which NRC has direct oversight are considered to be sub-components of the NRC LAN/WAN, only the physical and environmental controls and the personnel security controls were evaluated for these systems. The results were incorporated into the self-assessment for one of the agency's general support systems. The fourth contactor system for which the agency has direct oversight was expected to be certified and accredited in FY 2007, so the agency did not conduct a separate self-assessment for this system. However, the certification and accreditation was not expected to be completed prior to the submission of this report, so it was not originally included in the total number of contractor systems for which security controls have been tested and evaluated in the past year. Subsequent to the completion of fieldwork, the agency completed certification and accreditation of this system, and the system was granted an ATO.

For the seven contractor systems that are operated by other Federal agencies, NRC's policy is to confirm with the owner agencies that annual security control testing and evaluation has been completed. As two of the Federal contractor systems were just certified and accredited in FY 2007, these two systems were included in the total number of contractor systems for which security controls have been tested and evaluated. The agency has not obtained confirmation from the owner agencies of the other five contractor systems operated by other Federal agencies that annual security control testing and evaluation has been completed. Subsequent to the completion of fieldwork, the agency provided a certification memorandum for one of the Federal contractor systems that indicates security control testing and evaluation for the system was completed in FY 2007. However, the agency could not demonstrate that this system has been

[9] Management controls are the safeguards or countermeasures that focus on the management of risk and the management of information system security. Operational controls are the safeguards or countermeasures that primarily are implemented and executed by people (as opposed to systems). Technical controls are the safeguards or countermeasures that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

accredited (and therefore, that the designated approving authority for that system approved the testing and evaluation). Therefore, it was not included in the total number of contractor systems for which security controls have been tested and evaluated in the past year. As discussed later in Section 3.3 of this report, the FY 2005 and FY 2006 FISMA independent evaluation found that the agency does not maintain documentation that demonstrates that systems provided by other Federal agencies meet FISMA requirements.

The agency provided the majority of the self-assessments after the cutoff date established at the entrance conference, giving us only enough time to perform a cursory review. However, even a cursory review found that (1) the agency did not follow OMB and NIST guidance for conducting its annual security control assessments, (2) self-assessments were not always based on approved security categorizations, and (3) self-assessments contained errors and inconsistencies.

<u>Security Control Test and Evaluation – Background</u>

FISMA (section 3544(b)(5)) requires each agency to perform for all systems (including those operated by a contractor or other organization on behalf of an agency) "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but not less than annually." This review shall include the testing of management, operational, and technical controls, and is also referred to as a self-assessment.

The FY 2006 FISMA guidance stated that for FY 2007 and beyond, agencies will be required to use FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53 for the specification of security controls, and NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, for the annual assessment of security control effectiveness. After FY 2006, NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, is not to be used for the specification and/or assessment of security controls. This requirement was reiterated in the FY 2007 FISMA guidance, issued July 25, 2007.

In February 2007 (updated in May 2007), NIST issued a memorandum for the record stating that after the final release of NIST SP 800-53A in FY 2007 (tentatively scheduled for December 2007), NIST plans to rescind NIST SP 800-26. The memorandum also reiterated OMB's statement that for FY 2007 and beyond, agencies will be required to use NIST SP 800-53A for the assessment of security control effectiveness. Attached to the memorandum is a security controls assessment form, which replaces the form contained in NIST SP 800-26, and provides a standard methodology for capturing the results of system-level security control assessments. The form will be incorporated into the final release of NIST SP 800-53A. The memorandum stated that agencies may use the attached form to support security controls assessment requirements for FY 2007. The third public draft of NIST SP 800-53A was issued June 4, 2007.

<u>FINDING D – The Agency Did Not Follow OMB and NIST Guidance When Conducting Its Annual Self-Assessments (New Finding)</u>

Despite the requirement to use NIST SP 800-53A for the annual assessment of security control effectiveness, the agency conducted the FY 2007 self-assessments by using the approach of measuring progress by levels of effectiveness, as described in NIST SP 800-26. The agency also chose to use the self-assessment report format from NIST SP 800-26. The agency's methodology did not include all testing methods required by NIST SP 800-53A. As a result, the agency cannot be certain that all controls are operating as intended.

The agency's self-assessment methodology included the following activities:

- Sending a brief questionnaire to system owners to validate the system identification information and to request documents needed to support the self-assessment process.
- Reviewing existing documentation.
- If needed, sending additional questions to system owners.
- Interviewing system owners (some self-assessments were conducted without interviewing system owners).

The agency's security control assessment methodology is hierarchical and is based on the methodology described in NIST SP 800-26. The NIST SP 800-26 methodology comprises five levels to guide agency assessments. Level 1 indicates that there are policies in place for the security controls. Level 2 indicates that there are documented procedures for implementing the policies and the security controls. Level 3 indicates that the procedures and the security controls have been implemented. Level 4 indicates that procedures and controls are tested and reviewed. Finally, Level 5 indicates that procedures and controls are fully integrated into a comprehensive information system security program. Using the agency's methodology, if a control did not meet the requirements of a particular level, then the testing and evaluation of that control ended. For example, if a control had policies, but no procedures, then the implementation of that control was, in most cases, never evaluated, even if the control was actually implemented.

The security control assessment methodology described in NIST SP 800-53A is not hierarchical. NIST SP 800-53A describes three methods for assessing security controls: examine, interview, and test. These assessment methods are used to determine whether a particular security control is operating as intended (i.e., is the control implemented correctly, being used as intended, and producing the intended outcome with respect to meeting the security requirements for the information system). Control effectiveness is measured as satisfied, partially satisfied, or not satisfied. Satisfied indicates that the portion(s) of the security control being addressed by the procedural statement are operating as intended. Partially satisfied indicates that some portion(s) of the security control being addressed by the procedural statement are operating as intended, but other portions are not. Not satisfied indicates that the portion(s) of the security control being addressed by the procedural statement are not operating as intended. Using this methodology, a control without policies and/or procedures could still be found to be partially satisfied if the control was actually implemented as intended.

NIST SP 800-53A includes an assessment procedure catalog that specifies which assessment methods should be used to evaluate a particular security control. All assessment methods specified for a control in the assessment catalog are expected to be completed. For example, for the physical and environmental control PE-3 (physical access control), NIST SP 800-53A specifies that for a moderate-impact system, all three assessment methods – examine, interview, and test – should be used to test this control.

The agency's methodology included two of the assessment methods described in NIST SP 800-53A – examine and interview. However, due to the hierarchical nature of its process, not all of the assessment methods specified in the NIST SP 800-53A assessment catalog were performed for each control. Continuing with the PE-3 control example, the agency did not perform the test assessment method specified by NIST SP 800-53A for this control for the agency's remote locations. The agency stated that the physical and environmental controls for these locations had only policies in place (Level 1). Therefore, site visits were not necessary as they would be needed only to test the implementation (Level 3) of the control. Because the implementation of these controls was never tested, it is not possible to determine if the Level 1 effectiveness means there are no procedures and the control is not implemented, or if the control is implemented, but because there were no procedures, its implementation was never tested. As a result of the incomplete testing, the agency cannot be certain that all controls are operating as intended.

RECOMMENDATION

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

3. Conduct annual self-assessments in accordance with current OMB and NIST guidance.

FINDING E – Self-Assessments Were Not Always Based on Approved Security Categorizations (New Finding)

Carson Associates also found that self-assessments for 15 of the agency's 30 operational systems, and for 3 contractor systems were not based on an approved security categorization. As stated previously in Section 3.1 of this report, security categorizations are necessary to (1) determine the appropriate set of minimum security controls to implement for a system, and (2) identify the correct minimum security control baseline from NIST SP 800-53 to use when performing annual security control testing and review.

In some cases, we found that the impact levels for confidentiality, integrity, and availability noted on these self-assessments differed from the impact levels on the FY 2006 self-assessments, yet there is no explanation for the differences. For example, one system was evaluated against the low-impact security control baseline in FY 2007, but was evaluated against the moderate-impact security control baseline in FY 2006. Another system was evaluated against the high-impact security control baseline in FY 2006, but was evaluated against the moderate-impact security control baseline in FY 2007. Self-assessments that are not based on an approved security categorization may not be evaluating the appropriate set of controls. As a result, the agency cannot be certain that all controls are operating as intended.

RECOMMENDATION

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

4. For self-assessments conducted on systems without an approved security categorization, include an explanation as to how the impact levels for confidentiality, integrity, and availability were determined. This explanation should also include a discussion of any changes to the impact levels (if any) from the previous year's self-assessment.

FINDING F – Self-Assessments Contained Errors and Inconsistencies (New Finding)

Carson Associates also found the following errors and inconsistencies in the FY 2007 self-assessments:

- The blank self-assessment (template) for the moderate-impact baseline and all moderate-impact self-assessments are missing control identification and authentication control IA-2, enhancement 1.
- The blank self-assessment (template) for the high-impact baseline and all high-impact self-assessments include system and information integrity control SI-4, enhancement 1. This control is not part of the high-impact baseline.
- The self-assessment for one system with an approved security categorization has risk assessment control RA-2 (security categorization) incorrectly marked at Level 2 (procedures) when it should be marked at Level 3 (implemented).
- The self-assessments for six systems without approved security categorizations have control RA-2 incorrectly marked at Level 3 (implemented) when it should be marked at Level 2 (procedures).
- The self-assessment for one system with a POA&M has certification, accreditation, and security assessments control CA-5 (POA&M) incorrectly marked at Level 2 (procedures), when it should be marked at Level 3 (implemented).
- The section of the self-assessment that lists connected systems is inaccurate or incomplete for several systems.

As a result of the errors and inconsistencies, the agency cannot be certain that all controls are operating as intended, and cannot be certain that the self-assessments reflect the actual security status of the systems.

RECOMMENDATION

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

5. Develop and implement quality assurance procedures for self-assessments.

3.2.3 Contingency Planning and Testing

OMB Requirement	OIG Response
2. For the total number of systems reviewed by component/bureau and FIPS system impact level for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy. *2.c. Number of systems for which contingency plans have been tested in accordance with policy.*	*See Table 3-5 below.*

Table 3-5. Number of Systems With Tested Contingency Plans by FIPS 199 Risk Impact Level[10]

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	0	0	0
Moderate	5	2	7
Low	0	0	0
Not Categorized	0	0	0
Total	5	2	7

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, states that contingency plans should be tested at least annually and when significant changes are made to the information system, supported business process(s), or the contingency plan. Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, states that the NRC shall comply with the NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, IT risk assessments, and IT contingency plans), and other applicable NIST automated information security guidance for IT security processes, procedures, and testing. MD 12.5 also states that IT contingency plans for major applications and general support systems shall be tested each year. A live test provides the best indication of the adequacy of a contingency plan test. If a live test cannot be conducted due to operational constraints, a simulated test may be conducted in lieu of the live test. Information System Security (ISS) Security Procedure ISS-00-001, Revision 0, *Annual Update of System Security Documentation for Automated Information Systems*, dated March 1, 2006, also requires annual contingency plan testing for all major applications and general support systems, including the generation of a contingency plan test report.

[10] Any testing performed between October 1, 2006, and the completion of fieldwork, would be considered as FY 2007 test results. The testing itself must have occurred in that time frame. If the testing occurred prior to October 1, 2006, but the report was not submitted to/approved by the agency until after October 1, 2006, it would still be considered an FY 2006 test, and not an FY 2007 test. Only testing that is supported by a submitted and approved report will be counted.

FINDING G – Annual Contingency Plan Testing Is Still Not Being Performed For All Systems (Repeat Significant Deficiency)

This is a repeat finding from the FY 2005 and FY 2006 FISMA independent evaluations. Despite the requirement that contingency plans should be tested at least annually, only 5 of the agency's 30 operational information systems, and 1 of the agency's contractor systems, had its contingency plan tested in FY 2007. Subsequent to the completion of fieldwork, the agency provided documentation demonstrating that contingency plan testing was conducted for another contractor system; however, the agency has not yet received the test results report.

As a result, the agency has limited assurance that it will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption. Even a minor interruption could result in lost or incorrectly processed data if the contingency plan has not been tested.

In FY 2005, a recommendation was made to develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of a system's certification and accreditation. At the end of October 2006, the agency reported to the Commission that the Office of Information Services (OIS) would provide support to system owners (1) to complete the requirement to update their system's contingency plan, (2) to perform a contingency test in accordance with the contingency plan, and (3) to report on the results of the contingency test by June 1, 2007. However, in a November 2006, status update the agency stated that resources have not been available to support completion of annual contingency plan testing (including test reporting and contingency plan update) and that the target date for completing contingency plan testing for all agency systems was August 1, 2007. This target date was not met, despite the award of a consolidated information system security services contract in July 2006, which includes supporting the offices in completion of contingency plan updates and testing. The 3rd Quarter FY 2007 POA&M submitted to OMB has projected completion dates for contingency plan testing as late as the 4th Quarter FY 2009.

The following is a summary of the status of contingency plan testing for the 25 operational NRC systems that have not completed contingency plan testing in FY 2007:

- Five systems have never had their contingency plans tested.
- Two systems have never had their contingency plans tested, as they are new general support systems identified when the NRC local area network/wide area network (LAN/WAN) was divided into several general support systems. There is insufficient documentation to determine whether these systems were covered by previous LAN/WAN contingency plan tests.
- One system has not had its contingency plan tested in over 4 years.
- Thirteen systems have not had their contingency plans tested in over 3 years. Many of these systems are general support systems that were identified when the LAN/WAN was divided into several general support systems. There is insufficient documentation to determine whether these systems were fully covered by previous LAN/WAN contingency plan tests.

- Two systems had their contingency plans tested in 2005.
- Two systems had their contingency plans tested in 2006; however, the agency never approved the results for one of those systems.

The following is a summary of the status of contingency plan testing for the nine contractor systems that have not completed contingency plan testing in FY 2007:

- Five systems are operated by other Federal agencies. NRC is responsible only for confirming with the owner agency that annual contingency plan testing has been completed.
- Three systems have never had their contingency plans tested. While these are contractor systems, NRC is responsible for ensuring they have tested contingency plans.
- One system had its contingency plan tested in FY 2006.

See Appendix B of this report for details on the status of contingency plan testing for all agency and contractor operational systems.

As stated previously, OMB defines a significant deficiency as "a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets."

FISMA defines eight primary components of an agency's information system security program, including (1) annual testing of management, operational, and technical controls of every information system identified in the agency's inventory, and (2) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

The testing of contingency plans is a key element of the two information system security program components described above. It is essential for determining whether plans will function as intended in an emergency situation. Without testing, the agency has limited assurance that it will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption. Even a minor interruption could result in lost or incorrectly processed data if the contingency plan has not been tested.

In accordance with OMB requirements, the fact that the agency has failed to conduct annual contingency plan testing for all systems for the past 3 years constitutes a ***significant deficiency***. This deficiency is not a recent problem and the agency has made little progress in correcting the deficiency. According to the agency, completion of all contingency plan testing is not anticipated for at least another 2 years.

<u>RECOMMENDATION</u>

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

6. Develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of the systems' certification and accreditation. This recommendation replaces recommendation #3 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

3.3 Evaluation of Agency Oversight of Contractor Systems

OMB Requirement	OIG Response
3.a. The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	*Mostly (81-95% of the time)*

FISMA requires agencies to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (1) information collected or maintained by or on behalf of the agency and (2) information systems used or operated by an agency or other organization on behalf of an agency.[11]

NRC has a total of 11 systems operated by a contractor or other organization on behalf of the agency (8 major applications and 3 general support systems). Of the 11, 6 are operated by other Federal agencies, 2 are operated by federally funded research and development centers, and 3 are operated by contractors supporting the agency. NRC is responsible for direct oversight for four of these systems. Oversight of the remaining seven systems is the responsibility of the Federal agency operating the system.

<u>FINDING H – Agency Does Not Maintain Documentation That Demonstrates Systems Provided By Other Federal Agencies Meet FISMA Requirements (Repeat Finding)</u>

As in FY 2005 and FY 2006, Carson Associates found that the agency is still not maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements. As a result, the agency cannot be certain that the information security protections in place for these systems are commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information systems.

The agency has been working with the offices to assist in acquiring the required documentation for systems provided by other Federal agencies. However, according to the agency, some of the

[11] Information systems used or operated by a contractor of an agency or other organization on behalf of the agency refers to information systems that the agency considers to be either major applications or general support systems.

other Federal agencies have been unwilling to provide documentation that demonstrates they meet FISMA requirements. The other Federal agencies have also been unwilling to share copies of their annual self-assessments or results from their annual contingency plan testing. The OIG stated that a memorandum from the Federal agencies stating that annual self-assessments and annual contingency plan testing have been completed would be sufficient to meet the intent of the recommendations from the FY 2005 FISMA independent evaluation regarding this finding. The agency is currently working towards obtaining such memoranda. As of September 1, 2007, the agency had received certification and accreditation memoranda for only four of the seven systems provided or operated by other Federal agencies. Due to the current focus on the certification and accreditation phase of systems and scarcity of resources, the anticipated completion date to receive the rest of the required documentation for systems provided or operated by other Federal agencies is December 31, 2007.

RECOMMENDATION

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

7. Maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements. This recommendation replaces recommendations #4, #5, and #6 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

FINDING I – Oversight of Other Contractor Systems Is Lacking (Repeat Finding)

As in FY 2005 and FY 2006, Carson Associates found that oversight of other contractor systems still is lacking. Of the 11 systems operated by a contractor or other organization on behalf of the agency, NRC has direct responsibility for oversight of four of these systems. The agency has demonstrated proper oversight over only one of these systems. This system was issued an ATO shortly after the completion of fieldwork for this report. Certification and accreditation for one system is not scheduled to occur until the 1st Quarter FY 2008, and not until the 2nd Quarter FY 2009 for another system. The certification and accreditation for the third system has not been scheduled to date. As a result, the agency cannot be certain that the information security protections in place for these systems are commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information systems.

In a November 2006 status update, the agency stated that it was in the process of developing procedures for performing oversight of major applications and general support systems operated by a contractor or other operation on behalf of the agency. The agency anticipated completion and distribution of the procedures no later that December 29, 2006. In a subsequent update in July 2007, the agency stated that the procedures could be found in Section 4.2 and 4.4 of ISS Security Procedure ISS-00-001. While this document does describe the FISMA requirements for contractor systems, the agency has failed to actually implement those requirements for three contractor systems.

RECOMMENDATION

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

8. Develop and implement procedures for performing oversight of major applications and general support systems operated by a contractor or other organization on behalf of the agency. This recommendation replaces recommendation #7 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

3.4 Evaluation of Quality of Agency System Inventory

OMB Requirement	OIG Response
3.b. The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.	*Inventory is 81-95% complete*
3.c. The IG generally agrees with the Chief Information Officer (CIO) on the number of agency owned systems.	*Yes*
3.d. The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	*Yes*
3.e. The agency inventory is maintained and updated at least annually.	*Yes*
3.f. If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by component/bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.	*N/A (none missing)*

FISMA requires agencies to develop and maintain an inventory of major information systems operated by or under control of the agency. The inventory must include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. The inventory must be updated at least annually and must also be used to support information resources management. MD and Handbook 12.5 also require all interfaces to be included in the inventory, including interfaces with systems or networks not operated by or under the control of the agency.

While FISMA requires agencies to maintain an inventory only of major information systems (major applications and general support systems), NRC also tracks two other system types in its inventories – listed and other.

- **Listed** – a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which is not a major application or general support system when viewed from an agency perspective. Sensitive data may include individual Privacy Act information, law enforcement sensitive information, sensitive contractual and financial information, safeguards, and classified information. Listed systems would be considered minor applications using NIST terminology.[12]
- **Other** – an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC LAN/WAN.

To address findings from the FY 2005 FISMA independent evaluation regarding the agency's inventory, OIS developed a new centralized system for tracking NRC information systems. Data from various databases were compared, and any differences were resolved. The new system was then updated with data from biannual data calls, starting in September 2006. The new system continues to be updated with subsequent data calls. The agency also developed several procedures and guides to assist NRC offices with the biannual data call and to assist the agency in maintaining the inventory data in the new system.

Carson Associates found small discrepancies between the inventory of major applications, general support systems, and contractor systems reported in the metrics to OMB, and the actual contents of the agency's new inventory system. The agency has been made aware of these minor discrepancies and is working to correct them. Carson Associates also found that the agency is still in the process of populating the new inventory system with information on interfaces between systems.

The agency is also still working to complete one recommendation from the FY 2006 FISMA independent evaluation regarding the classification of the agency's Network Continuity of Operations (COOP) system. This system was categorized as a listed system, when it should have been categorized as a general support system. The agency has incorporated the components of the COOP system into existing infrastructure general support systems, and is no longer tracking the COOP system as an individual system. The agency has updated the security categorization documents for four general support systems to incorporate the appropriate COOP components, but they have not all been approved by the Senior Agency Information Security Officer.

RECOMMENDATION

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

9. Complete the updates to the security categorizations of the general support systems into which the Network Continuity of Operations system components have been incorporated. This recommendation replaces recommendation #2 from OIG-06-A-26, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2006*.

[12] An application, other than a major application, that requires 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. Minor applications are typically included as part of a general support system.

FINDING J – Agency Methodology Is Flawed for Identifying Which Listed Systems Reside On the NRC Network and Which Do Not (New Finding)

As stated previously, NRC tracks two other system types in its inventories – listed and other. For the purposed of certification and accreditation, the agency further categorizes listed systems as either networked (i.e., reside on the NRC network) or not networked (i.e., do not reside on the NRC network – systems that stand alone, and/or process safeguards information or classified data). The agency has different certification and accreditation requirements for listed systems that reside on the NRC network and for listed systems that do not reside on the network. However, the new inventory system does not provide a means to clearly distinguish which listed systems reside on the NRC network and which do not. The new inventory system has fields that are used to indicate the types of sensitive data processed by the system (e.g., safeguards information, Confidential, Secret, Top Secret, etc.). These fields could be used to infer whether or not a system resides on the network – that is, any system that processes these types of sensitive data cannot reside on the network. However, if the information in these fields is incorrect or incomplete, the agency has no other means of determining whether or not a listed system resides on the network. As a result, the agency may not be developing the appropriate certification and accreditation documentation for listed systems.

RECOMMENDATION

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

10. Develop and implement a methodology for identifying which listed systems reside on the NRC network and which do not.

3.5 Evaluation of Agency POA&M Process

OMB Requirement	OIG Response
4.a. The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	*Almost Always (96-100% of the time)*
4.b. When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	*Almost Always (96-100% of the time)*
4.c. Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	*Almost Always (96-100% of the time)*
4.d. Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	*Almost Always (96-100% of the time)*
4.e. IG findings are incorporated into the POA&M process.	*Almost Always (96-100% of the time)*

OMB Requirement	OIG Response
4.f. POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	*Almost Always (96-100% of the time)*

NRC has two primary tools for tracking IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. At a high level, NRC uses the POA&Ms required by OMB to track (1) corrective actions from the OIG annual independent evaluation, (2) corrective actions from the agency's annual review, and (3) recurring FISMA and IT security action items such as annual self-assessments and annual contingency plan testing. The POA&Ms may also include corrective actions resulting from other security studies conducted by or on behalf of NRC.

The more specific corrective actions associated with the certification and accreditation process (e.g., corrective actions resulting from risk assessments and security test and evaluation) are tracked in Rational® ClearQuest® as change requests using the project management methodology process for change management. All certification and accreditation corrective actions arising from the security test and evaluation process and from vulnerability scans are imported into Rational ClearQuest. A corrective action plan is generated directly from Rational ClearQuest. System owners are responsible for remediation of each corrective action within the timeframes specified in the corrective action plan using the project management methodology process for change requests.

Procedures for tracking and updating POA&Ms are provided to system owners with the biannual data call and when the agency requests updates to POA&Ms on alternate quarters between the biannual data calls. The project management methodology Web site provides detailed instructions on completing the corrective action plan.

The agency has made minimal progress in correcting weaknesses reported on its POA&Ms. The agency has corrected 35 percent of its program level weaknesses and 23.7 percent of its system level weaknesses. This is only a slight improvement over FY 2006. The majority of delays have been caused by delays in completing certifications and accreditations, as described later in this report, in Section 3.7. Refer to Appendix C of this report for a detailed analysis of the POA&Ms submitted for the first three quarters of FY 2007.

FINDING K – The Quality of the Agency's POA&Ms Needs Improvement (New Finding)

In assessing the agency's POA&M process, Carson Associates found that (1) the metrics submitted to OMB often deviated from the actual POA&Ms, and (2) the agency is not always following OMB and internal NRC POA&M guidance.

Metrics Submitted to OMB Deviate From the Actual POA&Ms

As in FY 2005 and FY 2006, Carson Associates found discrepancies between the metrics submitted to OMB and the actual POA&Ms. In previous FISMA evaluations, the discrepancies in the metrics were not considered significant enough to report as a weakness. However, we continue to find these discrepancies, and as a result, the agency may not be conveying an accurate picture of the agency's POA&M process and progress to OMB. The most common errors resulting in the discrepancies are:

- Counting weaknesses as closed in more than one quarter.
- Counting weaknesses as closed when they have not been closed by the OIG.
  - On the 2nd Quarter FY 2007 POA&M, the agency reported 11 weaknesses from OIG reports as completed when the OIG still considered the weaknesses as resolved[13] but not yet closed.
  - On the 3rd Quarter FY 2007 POA&M, the agency reported two weaknesses from OIG reports as completed when the OIG still considered the weaknesses as resolved but not yet closed.
- Not counting weaknesses as closed when they have been closed by the OIG prior to the cutoff date for POA&M reporting.
- Reporting weaknesses as on track when they are actually delayed.
- Reporting weaknesses as delayed when they are still on track.

The Agency Is Not Always Following OMB and NRC Internal POA&M Guidance

As in previous FISMA evaluations, Carson Associates also found that the agency is not always following OMB's POA&M guidance. The agency is also not following NRC internal POA&M guidance. The following are some examples of deviations from OMB and NRC internal POA&M guidance found on the FY 2007 POA&Ms.

- Weaknesses with completion dates over a year old are not always removed from the POA&Ms.
- Weakness with changes made to Schedule Completion Dates.
- Weaknesses with changes to Changes to Milestones (previously reported milestone changes were removed).

RECOMMENDATION

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

11. Develop and implement quality assurance procedures for POA&Ms.

[13] The OIG uses the term "resolved" to refer to a recommendation when it concurs with the agency's proposed actions to address to the recommendation, but the agency has not completed those actions to close the recommendation.

3.6 IG Assessment of the Certification and Accreditation Process

OMB Requirement	OIG Response
5.a. The IG rates the overall quality of the Agency's certification and accreditation process as:	*Failing*
5.b. The IG's quality rating included or considered the following aspects of the C&A process:	
Security plan	*X*
System impact level	*X*
System test and evaluation	*X*
Security control testing	*X*
Incident handling	*No (evaluated at the agency level)*
Security awareness training	*No (evaluated at the agency level)*
Configurations/patching	*X*
Other	*Risk assessment X*

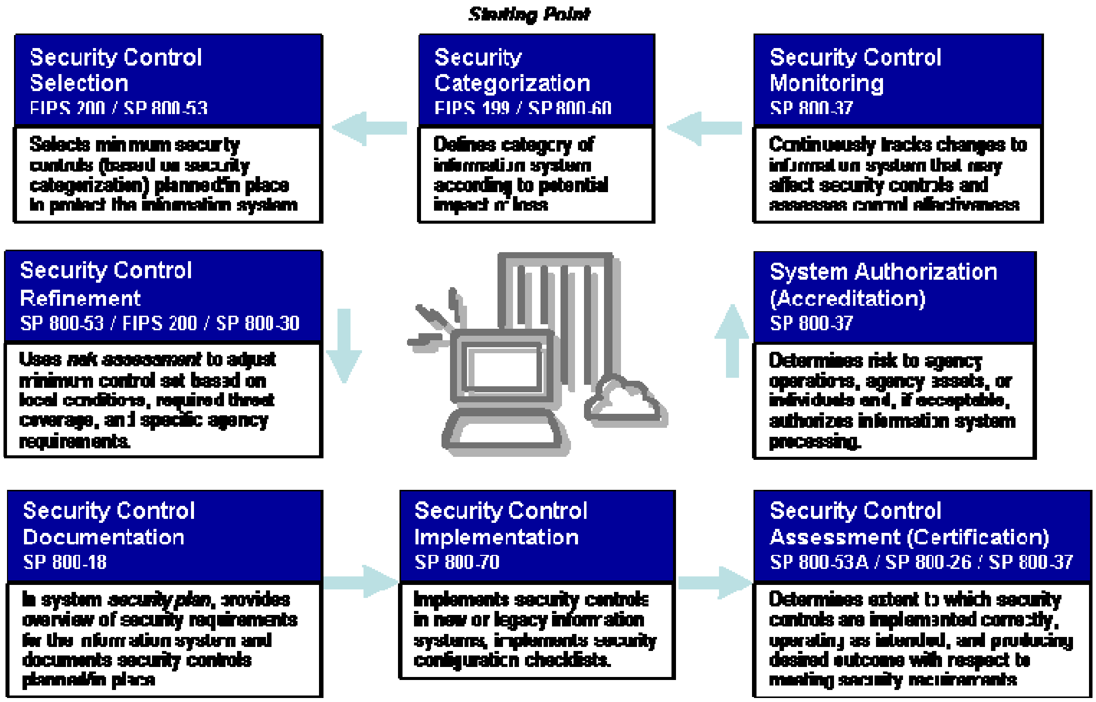
This section reports on Carson Associate's assessment of the agency's certification and accreditation process in detail. Section 3.2.1 of this report discusses the actual number of agency and contractor systems with a current certification and accreditation. In order to evaluate the agency's certification and accreditation process, Carson Associates evaluated the certification and accreditation documents for one of the two systems with a current certification and accreditation. We also reviewed the new certification and accreditation process and procedures located on the agency's project management methodology Web site, and reviewed accreditation decision memoranda issued by the agency's authorizing official. We rated the overall quality of the agency's certification and accreditation process as failing because the agency has completed the certification and accreditation of only two agency systems and one contractor system for which the agency has direct oversight in the past 2 years. The failing rating does not necessarily reflect the actual quality of the process itself. Carson Associates could not perform a complete evaluation of the agency's new certification and accreditation process, as only two systems had completed certification and accreditation under the new process at the time of our evaluation. Based on the certification and accreditation documents we did review, we found that the agency's certification and accreditation process is inconsistent with NIST guidance.

Certification and Accreditation – Background

The security certification and accreditation of information systems is integral to an agency's information security program and is an important activity that supports the risk management process required by FISMA. Information systems under development must be certified and accredited prior to becoming operational. Operational information systems must be re-certified and re-accredited every 3 years in accordance with Federal policy,[14] and whenever there is a significant change[15] to the information system or its operational environment.

The following diagram[16] illustrates the key activities, including certification and accreditation, in managing enterprise-level risk, i.e., risk resulting from the operation of an information system. As illustrated in the diagram, NIST has developed several standards and guidelines to support the management of enterprise risk. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for certification and accreditation.

Managing Enterprise Risk – The Framework



Security Control Selection
FIPS 200 / SP 800-53
Selects minimum security controls (based on security categorization) planned/in place to protect the information system

Security Categorization
FIPS 199 / SP 800-60
Defines category of information system according to potential impact of loss

Security Control Monitoring
SP 800-37
Continuously tracks changes to information system that may affect security controls and assesses control effectiveness

Security Control Refinement
SP 800-53 / FIPS 200 / SP 800-30
Uses *risk assessment* to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements.

System Authorization (Accreditation)
SP 800-37
Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing.

Security Control Documentation
SP 800-18
In system *security plan*, provides overview of security requirements for the information system and documents security controls planned/in place

Security Control Implementation
SP 800-70
Implements security controls in new or legacy information systems; implements security configuration checklists.

Security Control Assessment (Certification)
SP 800-53A / SP 800-26 / SP 800-37
Determines extent to which security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

Security *certification* is a comprehensive assessment of the management, operational, and technical security controls that are planned or in place in an information system to determine the extent to which the controls are (1) implemented correctly, (2) operating as intended, and (3) producing the desired outcome with respect to meeting the security requirements for the information system. The results of a security certification are used to reassess the risks and

[14] OMB Circular A-130, Appendix III.

[15] Examples of significant changes to an information system that should be reviewed for possible re-accreditation include (1) installation of a new or upgraded operating system, middleware component, or application; (2) modifications to system ports, protocols, or services; (3) installation of a new or upgraded hardware platform or firmware component; and (4) modifications to cryptographic modules or services. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the system security and trigger a re-accreditation action.

[16] The diagram was adapted from a diagram found in the NIST presentation "Building More Secure Information Systems: A Strategy for Effectively Applying the Provisions of FISMA," dated July 29, 2005 (http://csrc.nist.gov/sec-cert/PPT/fisma-overview-July29-2005.ppt).

update the system security plan, thus providing the factual basis for an authorizing official[17] to render a security accreditation decision. Security certification can include a variety of assessment methods (e.g., interviewing, inspecting, studying, testing, demonstrating, and analyzing) and associated assessment procedures depending on the depth and breadth of assessment required by the agency.

Security *accreditation* is the official management decision given by a senior agency official to (1) authorize operation of an information system and (2) explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. By accrediting an information system, an agency official accepts responsibility for the information system's security.

There are three types of accreditation decisions that can be rendered by authorizing officials: (1) ATO, (2) interim authorization to operate (IATO), and (3) denial of authorization to operate.

- **Authorization to Operate –** issued if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is acceptable.
- **Interim Authorization to Operate –** issued if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable, but there is an overarching mission necessity to place the information system into operation or continue its operation. An IATO is rendered when the security vulnerabilities identified in the information system (resulting from deficiencies in the planned or implemented security controls) are significant but can be addressed in a timely manner. An IATO provides a *limited* authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency for a specified period of time. In accordance with OMB policy, an information system is not *accredited* during the period of limited authorization to operate. The duration established for an IATO should be commensurate with the risk to agency operations, agency assets, or individuals associated with the operation of the information system. When the security-related deficiencies have been adequately addressed, the IATO should be lifted and the information system authorized to operate.
- **Denial of Authorization to Operate –** issued if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable. The information system is not accredited and should not be placed into operation. If the information system is currently operational, all activity should be halted.

The FY 2005 FISMA independent evaluation found that the majority of NRC information systems (19 of 27) were not certified and accredited because (1) the certification and accreditation had lapsed or was never completed and (2) NRC information systems were being re-certified and re-accredited using new NIST requirements.[18] As a result, potential risks to

[17] The agency refers to the authorizing official as the designated approving authority.

[18] NRC information systems are being re-certified and re-accredited in accordance with the minimum security controls for information systems defined in NIST SP 800-53.

agency information systems were unknown. Subsequent to the FY 2005 FISMA independent evaluation, the former Chairman directed the agency to submit a plan (1) to refocus the agency's FISMA program for FY 2006 and (2) for an independent review of NRC's FISMA program.

NRC Refocused Information System Security Program

Under the refocused program, the agency proposed performing certification and accreditation of systems that are a high priority from a mission perspective and others that potentially pose a higher security risk (e.g., agency systems that communicate with systems outside the NRC network). These high priority systems included legacy financial systems, two new systems, and infrastructure components supporting these high priority systems. In a February 2006 memorandum to office directors and regional administrators, the agency stated it planned to complete the certification and accreditation for the high priority systems by the first quarter of FY 2007.

The first phase of the refocused program also included the development of a new certification and accreditation process, which has been finalized. The agency has finalized the templates for all certification and accreditation documents as well as instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology. One of the agency's operational major applications was chosen to "pilot" the new process and documentation standards, in part, to ensure the new process is repeatable.

In response to the two significant deficiencies identified by the FY 2006 FISMA independent evaluation, the agency developed a plan to achieve full accreditation for 15 major applications/general support systems by August 30, 2007, and full accreditation of the remaining 15 major applications/general support systems by August 30, 2008. The agency's goal was to have six systems accredited by January 31, 2007. The agency did not meet this goal, and has changed the priorities of and schedule for the certification and accreditation efforts multiple times since the first schedule under the refocused program was issued in February 2006. As of the completion of fieldwork, the agency has completed the certification and accreditation of only two agency major applications/general support systems. The certification and accreditation for the system originally chosen to "pilot" the new process and documentation standards still has not been completed.

Even with the new certification and accreditation process, the refocused information system security program, and the award of a multi-year, multi-million dollar contract to provide the agency with consolidated information system security services, the agency has completed certification and accreditation of only two agency systems and one contractor system for which the agency has direct oversight in the past 2 years. In the meantime, the certifications and accreditations for all of the agency's remaining 28 operational systems have expired.

The FY 2005 FISMA independent evaluation made two recommendations to address the lack of certified and accredited systems: (1) develop and implement procedures for monitoring timely initiation of certification and accreditation efforts, and (2) develop and implement a mechanism for holding responsible managers and their staff accountable for completing certification and accreditation efforts in a timely manner. However, the agency is still in the process of implementing the first recommendation. According to the agency, the target date for developing and implementing procedures for monitoring timely initiation of certification and accreditation efforts was July 30, 2007. This target date was not met.

As stated previously, it constitutes a ***significant deficiency*** that only 2 of the 30 operational NRC information systems have a current certification and accreditation and only 5 of the 11 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation.

Independent Review of NRC's Information System Security Program

At the request of the former Chairman, the agency engaged outside expertise to perform an independent review of the adequacy of the agency's internal processes used to provide security to its information systems. NRC selected the Carnegie Mellon University's Software Engineering Institute to perform the independent review. Their approach to determining the adequacy of the agency's processes used to protect and secure its IT systems included the following tasks:

- Assist the NRC to understand the capability of its information system security program as compared to other similar-sized Government agencies, and assist the agency to improve its information system security program.
- Review the NRC certification and accreditation process to determine its consistency with NIST policies and guidance.
- Provide NRC leadership with guidance for certification and accreditation efforts, including benchmarks for cost, duration, resource commitment, and compliance reporting.

The final report was issued on November 13, 2006, and included 23 recommendations and 5 additional recommendations to consider. The agency submitted the report to the Commission on November 30, 2006, along with plans for addressing the recommendations made in the report. The agency stated that several recommendations address issues that span the agency's entire information security program, including functions residing in other offices. The agency also stated that the staff would provide an analysis of these issues along with options regarding the associated recommendations for Commission consideration in a separate Commission paper. The agency is currently working on developing a new security organization and reporting framework to address the implementation of these recommendations, but has not issued any further communication to the Commission on its progress.

FINDING L – The Agency's Certification and Accreditation Process Is Inconsistent With NIST Guidance (New Finding)

Carson Associates assessment of the agency's certification and accreditation process found that it is inconsistent with NIST guidance. Specifically we found that (1) the issuance of IATOs is still inconsistent with NIST guidance, and (2) certification and accreditation documents completed using the new procedures are inconsistent with NIST guidance.

Issuance of Interim Approvals To Operate Is Still Inconsistent With NIST Guidance

As stated previously, there are three types of accreditation decisions that can be rendered by authorizing officials: (1) an ATO, (2) an IATO, and (3) denial of authorization to operate. A full and complete certification and accreditation package is necessary for an authorizing official to render an accreditation decision. A complete certification and accreditation includes a security plan (which includes or references a risk assessment), a security assessment report, and a POA&M.

In prior years, the agency allowed current (legacy) systems to operate under an IATO prior to the completion of certification and accreditation, while concurrently pursuing authority to operate for new systems. However, OMB has clarified that allowing systems to operate under an IATO would not be an acceptable approach for the certification and accreditation of systems. NRC now bases the decision to issue an IATO on the submission of the following documents:

- NRC Form 616 – Notification of Electronic Information System Design or Modification
- NRC Form 637 – NRC Electronic Information System Records Scheduling Survey
- Privacy Impact Assessment
- Security Categorization (which includes an e-Authentication risk assessment)

Issuance of an IATO based on the submission of these documents is inconsistent with NIST guidance. None of these documents describe the actual risks that exist in the systems or identify threats and vulnerabilities that could expose the agency's information and information systems to an unacceptable level of risk. Such information is necessary for the authorizing official to determine whether the risk to agency operations, agency assets, or individuals, based on the implementation of an agreed-upon set of security controls for these systems, is acceptable.

The following is a summary of some of the agency's systems that are currently operating under an IATO.

- Three systems' last certification and accreditation expired more than 1 year ago.
- Two systems' last certification and accreditation expired more than 2 years ago.
- Two general support systems were identified when the LAN/WAN was divided into several general support systems. There is insufficient documentation to determine whether these systems are fully covered by the previous LAN/WAN certification and accreditation.
- One agency system has never had a complete certification and accreditation and does not even have a security plan or risk assessment.

The agency may have some understanding of the threats, vulnerabilities, and risks associated with the systems operating under an IATO that have (1) an expired certification and accreditation, (2) a risk assessment, or (3) a security plan. However, these documents are now outdated. As noted above, there are several systems operating under an IATO that have never had a risk assessment and do not have a security plan. For these systems, the authorizing official cannot make an informed decision regarding whether the risk to agency operations, agency assets, or individuals is acceptable.

As stated previously, the Software Engineering Institute evaluated the agency's certification and accreditation process. One of its recommendations was to make accreditation decisions based on a set of documents that provide an accurate identification and mitigation of risk, regardless of whether the authorizing official ultimately decides to grant an ATO, an IATO, or deny operation. The report also recommended that in addition to the security categorization, the agency should also require a system security plan prior to issuing an IATO. The agency stated in its response to the report that staff will ensure that the documentation upon which the accreditation is based contains an accurate identification of risk as well as any risk mitigation plans, and agreed that security plans should also be required.

However, the agency continues to issue IATOs without documentation that includes accurate identifications of risks, risk mitigation plans, or security plans.

RECOMMENDATION

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

12. Follow NIST guidance and only issue IATOs with documentation that includes accurate identification of risks, risk mitigation plans, and security plans.

Certification and Accreditation Documents Completed Using New Procedures Are Inconsistent With NIST Guidance

Carson Associates reviewed the certification and accreditation documents for one agency system that was completed using the new certification and accreditation process and templates. Our review found that several documents are inconsistent with NIST guidance.

Security Test and Evaluation

As stated earlier, NIST SP 800-37 provides guidance on the certification and accreditation process. In the security categorization phase, task 4, subtask 4.3 (security control assessment, security assessment) includes determining the extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. At the completion of task 4, the certification agent will be able to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The third phase of the certification and accreditation process is the security accreditation phase. The objective of task 6 of this phase (security accreditation decision) is to determine (1) the risk to agency operations, agency assets, or individuals and (2) if the agency-level risk is acceptable.

The system's security test and evaluation execution report stated that testing was limited to the 40 percent of the assurance controls selected by the NRC Senior Agency Information Security Officer for pre-approval to operate testing, and all of the functional security controls for the system. A total of 54 controls and 12 control enhancements stated as in-place in either the risk assessment or security plan were tested. However, 36 controls and 27 control enhancements stated as in-place were not tested. Some were hybrid controls, which are controls implemented by the system as well as by other systems, typically general support systems, which also provide that control. However, some were controls specific to the system being tested.

This is the first certification and accreditation for this system, so none of its security controls had been tested prior to the security test and evaluation conducted as part of the certification and accreditation. NIST SP 800-37 specifically states that the organization must assess all security controls in an information system during the initial security accreditation. If all of the security controls have not been tested, the certification agent cannot determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The authorizing official stated the following in the approval to operate memorandum for this system: "This security accreditation is my formal declaration that adequate security controls have been implemented in the information system and that a satisfactory level of security is present in the system." It is not possible to determine whether adequate security controls have been implemented if not all of the security controls have been tested.

Risk Assessment

In the security categorization phase, task 5, subtask 5.2 (security certification documentation, system security plan update) includes updating the system security plan (and risk assessment) based on the results of the security test and evaluation and any modifications to the security controls in the information system. At the completion of the security certification phase, the security plan and risk assessment should contain an accurate list and description of the security controls that are implemented (in place) and a list of identified vulnerabilities (i.e., controls that are not implemented or planned).

However, the system's risk assessment was not updated to reflect the results of the security test and evaluation. There were seven security controls and one enhancement that were determined to be not in place during the security test and evaluation. The risk assessment should have been updated to reflect that these controls are not in place, and the risks associated with the lack of these controls should have been re-evaluated.

Security Plan

NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, provides guidance for the development of security plans. Each control description should contain: (1) the security control title, (2) how the security control is being implemented or planned to be implemented, (3) any scoping guidance that has been applied and what type of consideration, and (4) indication of whether the security control is a common control and who is responsible for its implementation. The use of compensating controls should also be documented in the system security plan.[19]

[19] Compensating security controls are the management, operational, or technical controls employed by an agency in lieu of prescribed controls in the low, moderate, or high security control baselines, which provide equivalent or

The system's security plan makes no reference to scoping guidance that has been applied, and makes no specific mention of compensating controls. There are several controls that have had scoping guidance applied. For example, the access control AC-18 (wireless access restrictions) is noted as being not applicable. In this case, scoping guidance has been applied to remove this control from the moderate-impact baseline applied to the system. The security plan should have noted the type of scoping guidance – in this case, technology-related – that was applied to the control. There are also several controls that require compensating controls. There are eight controls and one control enhancement that are noted as "not planned" in the security plan. If these controls are not in place, and not planned, then there must be compensating controls in place to provide equivalent or comparable protection for the controls not in place.

RECOMMENDATION

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

13. Develop and implement quality assurance procedures to ensure certification and accreditation documentation is consistent with NIST guidance.

3.7 IG Assessment of Agency Privacy Program and Privacy Impact Assessment Process

3.7.1 Privacy Impact Assessment Process

OMB Requirement	OIG Response
6.a. Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, including adherence to existing policy, guidance, and standards.	*Excellent*

Carson Associates evaluated the agency's PIA process against the questions from the PIA and Web Privacy Policies and Processes section of the OMB Reporting Template for Senior Agency Officials for Privacy.

6.a.1. Does the agency have a written policy or process for determining whether a PIA is needed?

MD and Handbook 3.2, *Privacy Act*, requires office directors and regional administrators to ensure that PIAs are prepared and submitted to OIS before developing or procuring IT that collects, maintains, or disseminates personal information about individuals or when initiating a new electronic collection of personal information in identifiable form[20] from 10 or more persons. In accordance with the agency's project management methodology, a PIA is required for all investments at the inception phase of the development lifecycle. PIAs are also part of the

comparable protection for an information system. The use of compensating security controls must be reviewed, documented in the system security plan, and approved by the authorizing official for the information system.

[20] Information in identifiable form is information that permits the identity of the individual to whom the information applies to be reasonably inferred directly or indirectly.

agency's certification and accreditation process. ISS-01-001, Revision 0, *PIA Procedures*, dated August 30, 2006, requires a PIA (or update of an existing PIA) for each legacy system requiring re-certification and re-accreditation.

6.a.2. Does the agency have a written policy or process for conducting a PIA?

The agency has developed procedures (ISS-01-001) and a template for conducting PIAs. The procedures provide a detailed discussion of how to complete PIA and include guidance on how to complete certain questions on the PIA. MD and Handbook 3.2 require the OIS Business Process Improvement and Applications Division (BPIAD) Director to ensure that PIAs are conducted, reviewed, and approved before NRC collects information in an identifiable form or before developing or procuring IT that collects, maintains, or disseminates such information. The OIS Information and Records Services Division (IRSD) Director is required to ensure that PIAs are reviewed to address the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and records management requirements. Once IRSD has completed its review and approved a PIA, IRSD is responsible for declaring the PIA as an official agency record in agency's records management system.

6.a.3. Does the agency have a written policy or process for evaluating changes in business process or technology that the PIA indicates may be required?

PIAs are part of the agency's project management methodology and certification and accreditation process. Any changes in business process or technology indicated by a PIA would be handled in accordance with these processes.

6.a.4. Does the agency have a written policy or process for ensuring that system owners and privacy and IT experts participate in conducting the PIA?

Offices/system owners are responsible for preparing a PIA for each IT project/system they sponsor and submitting it to OIS for review and approval. The PIA undergoes review several times during development by privacy and IT experts, including the agency Privacy Program Officer, IRSD privacy and records staff, the computer security team, and the agency's Senior Agency Information Security Officer.

6.a.5. Does the agency have a written policy or process for making PIAs available to the public in the required circumstances?

6.a.6. Does the agency have a written policy or process for making PIAs available in other than required circumstances?

PIAs for systems that collect information from or about members of the public are made publicly available and posted on the NRC external Web, unless making the PIA public would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in the assessment. The sponsoring office is responsible for performing the review that determines if the PIA can be made public or not. Should an office wish to post a PIA on the external Web that does not collect information from or about members of the public, the office must inform the Privacy Program Officer that it has completed a review and that there is nothing in the PIA that would preclude it from being made public. The Privacy Program Officer changes the availability of the document in the agency's records management system and has it posted on the agency's external Web site.

6.a.5. Does the agency have a written policy or process for determining continued compliance with stated Web policies?

MD and Handbook 3.14, *U.S. Nuclear Regulatory Commission External Web Site*, include policies and procedures to ensure that (1) operation of the site complies with applicable laws and regulations, (2) all content on the external Web site contributes to increasing public confidence in the NRC and to making conducting business with the NRC more efficient and effective, and (3) the content (i) reflects agency policy; (ii) is accurate, current, and easy to find; (iii) is accessible by all site users, including those with disabilities; (iv) adheres to best practices for Web usability; (v) does not unfairly promote one organization or commercial entity over others; and (vi) is published only once and is referenced by links when the same content is related to more than one topic.

The MD and Handbook are augmented by additional guidance on the agency's internal Web site. The additional guidance includes interface requirements for Web-based software applications, requirements and best practices for Government Web managers, and information on who participates in Web publishing. The agency's process for publishing content to the agency's external Web site includes five basis steps: (1) initial authorization of content, (2) screening content, (3) preparing content, (4) formatting content, and (5) publishing content. During the screening step, the content is checked for Web suitability, and includes checks for copyright, OMB information collection requirements, persistent cookies, privacy, and sensitivity. The Web site includes numerous instructions and checklists for each step of the publishing process.

6.a.6. Does the agency have a written policy or process for requiring machine-readability of public-facing agency Web sites (i.e., use of P3P[21])?

As MD and Handbook MD 3.14 were last issued prior to the OMB memorandum requiring that privacy policies be translated into a standardized machine-readable format, the agency has posted this requirement on its internal Web site.

[21] The Platform for Privacy Preferences Project (P3P) enables Web sites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents.

3.7.2 Progress in Implementing OMB M-06-15

OMB Requirement	OIG Response
6.b. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information," since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).	*Excellent*

In its FY 2006 FISMA submission to OMB, the agency reported that in response to OMB M-06-15, it conducted a review of physical and personnel security, and administrative and technical policies and processes related to the prevention of the intentional or negligent misuse of, or unauthorized access to PII. Subsequent to that review, the agency has made significant progress in implementing the provisions of M-06-15 as well as subsequent memoranda issued by OMB regarding privacy and PII.

To ensure that all agency personnel are familiar with the requirements of the Privacy Act, the agency's implementing regulation, and any other special requirements (i.e., handling PII), NRC issues regular announcements to all employees. These announcements provide general guidance or address specific issues. Each notice directs agency personnel to an internal Privacy Act Web page which provides staff access to guidance, regulations, procedures, and training in the area of the Privacy Act. The agency has issued the following announcements regarding the Privacy Act and the protection of PII.

- NRC Yellow Announcement YA-06-0039, *Safeguarding Personal Privacy Information*, June 22, 2006
- NRC Yellow Announcement YA-06-0069, *Protection of Personally Identifiable Information*, September 19, 2006
- NRC Yellow Announcement YA-07-0071, *Privacy at the NRC*, July 18, 2007

The agency created a PII poster that has been displayed in all agency buildings. Smaller copies of the poster are displayed throughout agency offices. The agency also maintains a PII project Web page that describes the agency's activities related to the protection of PII. This Web page contains information such as (1) frequently asked questions; (2) how to report inadvertent releases of PII; (3) links to OMB, Office of Personnel Management, and NRC PII policy; (4) information on the agency's PII task force (e.g., background and charter, membership, and meeting minutes); and (5) information on automated tools available to assist in searching for files that contain PII.

In addition to the activities requested by OMB, NRC conducted a thorough review of documents in the public library of the agency's document management system to identify and secure any documents that contained a Social security number (SSN). The documents containing PII were removed from the public library immediately. All current and former NRC employees whose SSNs were available in the public library were notified. NRC is in the process of finalizing notification letters to the non-NRC entities who submitted the documents with SSNs to the public library. NRC is also working on identifying and notifying the non-NRC staff whose SSNs were made available in NRC correspondence. NRC also notified OMB and the Department of Homeland Security about the PII contained in documents placed in the public library of the agency's documents management system.

In response to OMB-06-16, *Protection of Sensitive Agency Information*, dated June 23, 2006, the agency implemented short-term plans to (1) focus on improving staff awareness, (2) review and update current direction to reflect the new OMB recommendations related to PII, and (3) assist offices in identifying current data sources with PII information. The agency's security awareness training was updated to reflect PII data requirements. The agency also created an interoffice task force to determine the business processes that include PII, including data collection resulting from NRC information collections and NRC forms, and to revise agency direction, as appropriate, on the use of PII. Other short-term plans include: (1) developing a detailed plan and schedule to complete a comprehensive review of the main and public libraries of the agency's documents management system to identify and secure documents containing PII other than SSNs; and (2) asking contract project managers to have current contractors inventory PII in their possession, and then determine the contractor's need to possess the PII.

Mid-term activities focus on implementing mitigation strategies to protect PII from unauthorized use. The agency is evaluating major systems that use PII, and is consolidating its automated inventory system in order to further ensure all systems that utilize PII have been identified and are appropriately managed. The agency is also developing mitigation techniques to eliminate PII where possible on agency systems identified or to ensure that PII is managed in a safe and secure manner.

Long-term goals include (1) updating MD and Handbook 12.5 to reflect to reflect PII direction; (2) identifying, protecting, and monitoring access to PII through completion of certification and accreditation of NRC's major systems; and (3) designing, developing, and implementing a uniform enterprise security architecture based upon Federal and commercial "best practices."

The agency has issued guidance on (1) the use of mobile computers and devices (NRC-owned and personally owned) to store PII, (2) the removal of paper documents that contain PII from NRC-controlled space, (3) the use of NRC remote access services to access systems containing PII, and (4) password-protection of mobile devices. The agency's remote access system invokes a forced logout after 30 minutes of user inactivity, and BlackBerry devices have a system-enforced logout after 15 minutes of inactivity.

As a result of a report issued by the OIG in FY 2006, the CIO directed offices to conduct an immediate review of all network drives for the presence of personal privacy information and remove any information that should not be posted on a network drive unless access to that information is appropriately restricted to users with a "need to know." OIS provided the offices with guidance, support, and an automated tool to assist the staff in searching and identifying documents with personal privacy information. This initial effort was completed in April 2007. The agency is still developing policies and procedures for performing periodic reviews of network drives for the presence of personal privacy information.

3.8 Configuration Management

OMB Requirement	OIG Response
7.a. Is there an agency-wide security configuration policy?	*Yes*
7.b. Approximate the extent to which applicable information systems apply common security configurations established by NIST.	*Rarely (0-50% of the time)*

The agency has implemented several policies that address security configurations and their implementation. System security screening guidelines were developed to prepare new systems for implementation into the NRC production operating environment. The security screening ensures that system configurations meet NRC network security requirements. The guidelines outline the steps necessary to request and perform the security screening process, provide guidance on managing and developing a secure system, and list industry best practices and additional resources.

The agency has also posted guidance on the NRC internal Web site requiring the use of hardening specifications for the different operating systems and software in use at the agency. Hardening specifications in use at the agency include benchmarks developed by the Center for Internet Security, the Defense Information Systems Agency (DISA) Gold Disk,[22] National Security Agency security configuration guides, and custom hardening specifications developed by the agency. The agency requires the use of the most recent version of the specified hardening specifications.

NRC uses PatchLink to keep desktop configurations consistent across NRC. Network Bulletins are used to announce agency workstation updates. The announcements describe the nature of the upgrade and whether or not a workstation restart is required after the patches are installed.

NRC also requires all new acquisitions to include language to ensure that information technology providers certify their products operate effectively using the common security configurations required by OMB memorandum M-07-18, *Ensuring New Acquisitions Include Common Security Configurations*.

Carson Associates could not fully determine the extent to which applicable information systems apply common security configurations established by NIST. The agency did not provide the list of NIST or NIST-approved configurations in use at the agency until the last day of fieldwork. There was insufficient time to select a representative set of information systems to compare against the stated security configurations for the various operating systems and software in use at the agency.

Carson Associates did review the security test and evaluation results for the agency system selected for evaluation in FY 2007. DISA Gold Disk scans of the servers that support this

[22] The DISA Gold Disk is a tool that allows a system administrator to scan a system for vulnerabilities, make appropriate security configuration changes, and apply security patches. The Gold Disk uses an automated process that configures a system in accordance with DISA Security Technical Implementation Guidelines.

system found that none of the servers were in compliance with the NRC-specified hardening specifications for those operating systems.

3.9 Incident Reporting

OMB Requirement	OIG Response
8.a. The agency follows documented policies and procedures for identifying and reporting incidents internally.	*Yes*
8.b. The agency follows documented policies and procedures for reporting to US-CERT.	*Yes*
8.c. The agency follows documented policies and procedures for reporting to law enforcement.	*Yes*

MD and Handbook 12.5, Appendix B, formalizes the agency's procedures for monitoring, detecting, reporting, and responding to information systems security incidents. It also provides the requirements and procedures for reporting incidents internally, for reporting to US-CERT,[23] and for reporting to law enforcement. The most current version of the incident response procedures is maintained on the agency's internal Web site.

The Management Directive defines the roles and responsibilities for reporting and responding to information system security incidents. When criminal activity is suspected or confirmed, the procedures assign the OIG responsibility for contacting and coordinating the response with law enforcement officials.

Carson Associates reviewed samples of various incident response reports to determine whether the agency follows documented policies and procedures for identifying and reporting incidents.

3.10 Security Awareness Training

OMB Requirement	OIG Response
9. Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?	*Almost Always (96-100% of employees)*
10. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	*Yes*

All new NRC employees (including contractors, interns, and summer hires) are required to attend orientation the first day they report for duty. During the orientation, a member of the NRC Computer Security Team gives a brief presentation, which includes a discussion on appropriate use of information technology equipment. In addition, a member of the Office of the

[23] The procedures actually reference reporting to the Federal Computer Incident Response Center, which was replaced with the US-CERT when the Department of Homeland Security was established.

General Counsel presents a session on ethics that includes additional discussions on appropriate use of the Internet.

For FY 2007, all employees, including contractors, were required to attend in-person IT security training to ensure all employees are aware of their personal IT security responsibilities. Training sessions took approximately 3 hours and were held between October 2006 and December 2006, with a few makeup sessions scheduled in early January 2007. Employees hired since these training sessions were over are required to watch a video of the course (either online or on DVD). As of April 2007, the agency had achieved 100-percent compliance. The agency used NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, and NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, for sources of topics for the training course. The presentation slides from the course, the participant manual, and the NRC User Responsibilities for IT Security Golden Book are available online on the NRC internal Web site. The agency has also posted questions and answers from the various training sessions on the NRC internal Web site.

All Information System Security Officers and IT managers are required to take an additional online IT security awareness training course in addition to the required security awareness training described above. This additional IT security awareness training course must be taken every 3 years. NRC also provides an online IT security awareness course for system administrators. All system administrators must take this training course before assuming their duties, and then every 3 years thereafter.

NRC meets the Office of Personnel Management requirement to expose employees to security awareness materials at least annually by (1) mandating all NRC staff take annual IT security awareness training and by documenting who takes the annual training; (2) using posters, flyers, Web pages, NRC Yellow Announcements,[24] NRC Announcements, and articles/notices in the NRC monthly newsletter to keep computer security on everyone's mind throughout the year; and (3) by holding an Annual NRC Security Awareness Day event.

The agency is in the process of developing a computer security awareness and training program plan to fully implement the requirements outlined in OMB Circular A-130, Appendix III; FISMA; Management Directive and Handbook 12.5; and the Office of Personnel Management's final regulations concerning information technology security awareness.

The FY 2007 in-person security awareness training included a discussion of the dangers of peer-to-peer applications such as instant messaging. The installation of peer-to-peer software on NRC computers without explicit written approval of the NRC designated approving authority is prohibited. The agency provides a peer-to-peer frequently asked questions document on its internal Web site.

[24] NRC Yellow Announcements (formerly Yellow Announcements) establish new policies, practices, or procedures; introduce changes in policy, senior staff assignments, or organization; or address major agencywide events. These announcements require signature and are retained as permanent records in the agency's document management system.

FINDING M – Agency Lacks Procedures for Ensuring Employees With Significant IT Security Responsibilities Receive Security Training (Repeat Finding)

While the agency meets the FISMA requirement to ensure all employees received IT security awareness training, the agency still has not met the requirement to provide specialized training for employees with significant security responsibilities as described in NIST SP 800-16.

The FY 2005 FISMA independent evaluation found that the agency had difficulty in gathering the information needed to report on (1) the total number of employees with significant IT security responsibilities, (2) the number of those employees who have received specialized training, and (3) the total cost for providing IT training. At the time of the FY 2005 FISMA independent evaluation, the agency's training system did not identify which employees have significant IT security responsibilities and what courses are considered related to IT security. The agency's training system also did not account for any training the employees may have taken on their own time.

The agency is working with NRC offices to identify employees and contractors with significant IT security responsibilities. The agency is also developing procedures for ensuring staff with significant IT security responsibilities are identified and receive security awareness training and that the individual and associated training are properly documented and readily identifiable. According to the agency, the current target date for completing the recommendation from the FY 2005 FISMA independent evaluation concerning security training for employees and contractors with significant IT security responsibilities is August 31, 2008.

RECOMMENDATION

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

14. Develop and implement procedures for ensuring employees and contractors with significant IT security responsibilities are identified, receive security awareness and training, and the individual and associated training are readily identifiable. This recommendation replaces recommendation #10 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

3.11 E-Authentication Risk Assessments

OMB Requirement	OIG Response
11. The agency has completed system e-authentication risk assessments.	*No*

In December 2003, OMB issued memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*. The guidance applies to remote authentication of users of Federal agency information technology systems for the purposes of conducting Government business electronically (or e-Government). Remote authentication occurs when users identify and authenticate to information systems from outside of a specified security perimeter that is considered to offer sufficient protection. Performing an e-authentication risk assessment can also assist agencies in determining the appropriate identification and authentication controls for their systems. In addition, the e-authentication initiative is the first reusable component of the Federal Enterprise Architecture, the second e-Government cross-cutting initiative. Part of the Federal Enterprise Architecture plan is that the vast majority of Federal systems incorporating authentication functions should migrate to support e-authentication over time.

The e-authentication risk assessment is also required to implement Part 2 FIPS 201-1, *Personal Identity Verification of Federal Employees and Contractors*, dated March 2006. In accordance with OMB M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 5, 2005, in order to implement Part 2 of the standard, by October 27, 2006, all departments and agencies must begin deploying products and operational systems meeting specific requirements, including the use of digital certificates. According to the OMB memorandum, agencies must require the use of the identity credential for system access. Agencies must prioritize this requirement based on risk, using their authentication risk assessments required by previous OMB guidance and the categorization required by FIPS 199.

While OMB M-04-04 only requires e-authentication risk assessments for e-Government systems, NRC requires e-authentication risk assessments for all agency systems that require security categorizations. The e-authentication risk assessment is conducted during the security categorization of a system.

FINDING N – E-Authentication Risk Assessments Have Not Been Completed (Repeat Finding)

This is a repeat finding from the FY 2005 and FY 2006 FISMA independent evaluations. The FY 2005 FISMA independent evaluation also found that the six e-authentication risk assessments that were completed at the time were incorrect and inconsistent with the systems' FIPS 199 security categorizations. The agency has completed all e-authentication risk assessments required under OMB M-04-04; however, the agency (1) has not completed e-authentication risk assessments for all agency systems in accordance with its own policy, and (2) has not completed their review and update of the six e-authentication risk assessments originally identified in FY 2005 as having inaccuracies and inconsistencies. Only 15 of the 30 operational NRC information systems have completed e-authentication risk assessments. Only 5 of the 11 contractor systems have completed e-authentication risk assessments. According to the agency, the target date for completing all e-authentication risk assessments was July 30, 2007. This target date was not met.

Not only is the agency failing to meet the requirement to complete e-authentication risk assessments, the agency also cannot prioritize the HSPD-12 and FIPS 201-1 requirement to use the identity credential for system access as not all systems have been categorized in accordance with FIPS 199, and not all systems have completed their authentication risk assessments.

RECOMMENDATION

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

15. Develop and implement a plan for completing the remaining e-authentication risk assessments. This plan should include the review and update of the remaining two e-authentication risk assessments originally identified in FY 2005 as having inaccuracies and inconsistencies. This recommendation replaces recommendations #8 and #9 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

4 Consolidated List of Recommendations

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

1. Review and correct as needed all security categorizations so that they consistently reflect the information types that reside on the systems.
2. Categorize all NRC major applications and general support systems in accordance with FIPS 199. This recommendation replaces recommendation #1 from OIG-05-A-21, *Independent Evaluation of NRC’s Implementation of FISMA for Fiscal Year 2005*.
3. Conduct annual self-assessments in accordance with current OMB and NIST guidance.
4. For self-assessments conducted on systems without an approved security categorization, include an explanation as to how the impact levels for confidentiality, integrity, and availability were determined. This explanation should also include a discussion of any changes to the impact levels (if any) from the previous year’s self-assessment.
5. Develop and implement quality assurance procedures for self-assessments.
6. Develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of the systems’ certification and accreditation. This recommendation replaces recommendation #3 from OIG-05-A-21, *Independent Evaluation of NRC’s Implementation of FISMA for Fiscal Year 2005*.
7. Maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements. This recommendation replaces recommendations #4, #5, and #6 from OIG-05-A-21, *Independent Evaluation of NRC’s Implementation of FISMA for Fiscal Year 2005*.
8. Develop and implement procedures for performing oversight of major applications and general support systems operated by a contractor or other organization on behalf of the agency. This recommendation replaces recommendation #7 from OIG-05-A-21, *Independent Evaluation of NRC’s Implementation of FISMA for Fiscal Year 2005*.
9. Complete the updates to the security categorizations of the general support systems into which the Network Continuity of Operations system components have been incorporated. This recommendation replaces recommendation #2 from OIG-06-A-26, *Independent Evaluation of NRC’s Implementation of FISMA for Fiscal Year 2006*.
10. Develop and implement a methodology for identifying which listed systems reside on the NRC network and which do not.
11. Develop and implement quality assurance procedures for POA&Ms.
12. Follow NIST guidance and only issue IATOs with documentation that includes accurate identification of risks, risk mitigation plans, and security plans.
13. Develop and implement quality assurance procedures to ensure certification and accreditation documentation is consistent with NIST guidance.
14. Develop and implement procedures for ensuring employees and contractors with significant IT security responsibilities are identified, receive security awareness and training, and the individual and associated training are readily identifiable. This recommendation replaces recommendation #10 from OIG-05-A-21, *Independent Evaluation of NRC’s Implementation of FISMA for Fiscal Year 2005*.

15. Develop and implement a plan for completing the remaining e-authentication risk assessments. This plan should include the review and update of the remaining two e-authentication risk assessments originally identified in FY 2005 as having inaccuracies and inconsistencies. This recommendation replaces recommendations #8 and #9 from OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

5 Agency Comments

At an exit conference with the agency held on September 17, 2007, the agency provided informal written comments and generally agreed with the report recommendations. The NRC Chief Information Officer provided a formal response to this report on September 24, 2007. Appendix E contains the Chief Information Officer's transmittal letter. The agency's formal comments along with OIG's analysis and response to those comments are included as Appendix F. This final report incorporates revisions made, where appropriate, in response to the agency's comments.

[Page intentionally left blank]

Appendix A. SCOPE AND METHODOLOGY

Carson Associates performed an independent evaluation of NRC's Implementation of FISMA for FY 2007. To conduct the independent evaluation, the team met with agency staff responsible for implementing the agency' information system security program, reviewed certification and documentation for the agency's operational information systems, and reviewed other documentation provided by the agency that demonstrated its implementation of FISMA.

All analyses were performed in accordance with guidance from the following:

- National Institute of Standards and Technology standards and guidelines
- Nuclear Regulatory Commission Management Directive and Handbook 12.5, *NRC Automated Information Security Program*
- NRC Office of the Inspector General audit guidance

This work was conducted between April 2007 and August 2007. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. The work was conducted by Jane M. Laroussi, CISSP, and Kelby M. Funn, CISA, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]

Appendix B. STATUS OF CONTINGENCY PLAN TESTING

The following information on the status of contingency plan testing was obtained from the 3rd Quarter FY 2007 POA&Ms submitted by the agency to OMB and from working papers from the FY 2007 FISMA independent evaluation. Systems with contingency plans tested in FY 2007 are indicated by shading in the "Last CP Test Date" column. Systems with contingency plan testing scheduled for FY 2007, but which have not yet completed contingency plan testing, are indicated by shading in the "Scheduled Test Date" column.

Table B-1. Status of Contingency Plan Testing

System	Last CP Test Date	Scheduled Test Date	Comment
Agency Systems			
3-Tier Web	Never tested	August 2008	
ADAMS	August 16, 2004	November 25, 2007	
CTF	June 29, 2004	November 30, 2007	Last test was "inherited" from LAN/WAN.
DCS	April 29, 2004	July 30, 2007	
DDMS	Between 6/28/07 and 7/25/07	Not yet scheduled	
Desktops	June 29, 2004	June 2008	Last test was "inherited" from LAN/WAN.
E-mail	June 29, 2004	Q4 FY 2009	Last test was "inherited" from LAN/WAN.
EHD	Never tested	June 30, 2007	
EIE	April 6, 2006	Q1 FY 2009	Agency never approved test results from April 2006.
ERDS	August 2007	Not yet scheduled	August 2007-Headquarters, January 2007-Regions I and III, February 2007-Region IV, March 2007-Region III.
Fees System	April 24, 2007	Not yet scheduled	
GLTS	May 13, 2004	Mid FY 2009	

System	Last CP Test Date	Scheduled Test Date	Comment
HPCS-CDS/CFD	Never tested	Q1 FY 2009	Transitioning to a listed system, so a contingency plan would not be required after the transition. However, the planned transition to listed system has not occurred.
HRMS	May 8, 2007	Not yet scheduled	
IDSSD	June 29, 2004	Q2 FY 2008	Last test was "inherited" from LAN/WAN.
IPSS	July 25, 2003	December 31, 2007	
LAN/WAN	May 10 and May 11, 2005	December 2008	Testing was just for switches and routers.
LTS	May 18, 2004	Q1 FY 2009	Was to be retired by September 30, 2005. As of the completion of fieldwork, the system had not been retired.
MPKI	June 29, 2004	July 15, 2008	Last test was "inherited" from LAN/WAN.
Novell Servers	June 29, 2004	August 30, 2008	Last test was "inherited" from LAN/WAN.
NSICD	Never tested	Q2 FY 2008	This system does not have a contingency plan.
OCIMS	June 19, 2006	September 30, 2007	
RAS	March 27, 2004	August 2008	This is another general support system that was broken out from the LAN/WAN. According to the agency, it was included with the continuity of operations testing performed in March 2004.
RPS	July 9, 2007 and July 13, 2007	Not yet scheduled	
SGI-LAN	Never tested – new system in FY 2007	Not yet scheduled	

System	Last CP Test Date	Scheduled Test Date	Comment
TAC	June 24, 2005	Q4 FY 2009	Planned transition to listed system (once HPCS moves to the production operating environment). Transition to listed system delayed until February 15, 2008.
Telecommunications	April 29, 2004	November 2008	
Unix Servers	Insufficient documentation to determine whether covered by previous tests	Q4 FY 2009	This is another general support system that was broken out from the LAN/WAN.
Web Servers	Insufficient documentation to determine whether covered by previous tests	June 1, 2006 (delayed, completion date to be determined)	This is another general support system that was broken out from the LAN/WAN.
Windows Servers	June 29, 2004	August 2009	Last test was "inherited" from LAN/WAN.
Contractor Systems			
CNWRA	Unknown	Unknown	
e-QIP	Unknown	Unknown	
FFS	March 2007	March 2008	
FPDS-NG	Unknown	Unknown	
FPPS	August 2007	August 2008	
INL	Unknown	Unknown	
L3-EER	Unknown	Unknown	
LMIT	Unknown	Unknown	
LSN	April 27-28, 2006	September 29, 2007	
NIH	Unknown	Unknown	
SPS	Unknown	Unknown	

ADAMS	Agencywide Document Access and Management System
CNWRA	Center for Nuclear Waste Regulatory Analyses
CTF	Consolidated Test Facility
DCS	Data Center Services
DDMS	Digital Data Management System

e-QIP	Electronic Questionnaire for Investigations Processing
EHD	Electronic Hearing Docket
EIE	Electronic Information Exchange
ERDS	Emergency Response Data System
Fees System	A group of nine applications that support the collection of license fees
FFS	Federal Financial System
FPDS-NG	Federal Procurement Data Systems-Next Generation
FPPS	Federal Personnel and Payroll System
GLTS	General License Tracking System
HPCS-CDS/CFD	High Performance Computing System – Code Development System/Computational Fluid Dynamics System
HRMS	Human Resources Management System
IDSSD	Intrusion Detection System and Security Devices
INL	Idaho National Laboratory
IPSS	Integrated Personnel Security System
L3-EER	L-3 Communications Corporation, Government Services, Inc.
LAN/WAN	Local Area Network/Wide Area Network
LMIT	Lockheed Martin Information Technology
LSN	Licensing Support Network
LTS	License Tracking System
MPKI	Managed Public Key Infrastructure
NIH	National Institutes of Health
NSICD	NRC Systems Inventory and Configuration Database
OCIMS	Operations Center Information Management System
RAS	Remote Access System
RPS	Reactor Program System
SGI-LAN	Safeguards Local Area Network (also referred to as Secure LAN)
SPS	Secure Payment System
TAC	Technology Assessment Center

Appendix C. DETAILED POA&Ms ANALYSIS

The agency carried over a total of 33 program level and 172 system level weaknesses from FY 2006 into FY 2007. The following tables provide statistics from the FY 2007 POA&Ms the agency has submitted to OMB for the 1st, 2nd, and 3rd quarters. These statistics reflect our analysis of the POA&Ms and may differ from the actual metrics submitted to OMB.

Table C-1. Program Level POA&M Statistics

Quarter	# At Start of Quarter	# New	# Completed	# Ongoing	# Delayed	# For Start of Next Quarter
Q1	33	5	0	16	22	38
Q2	38	2	9	17	14	31
Q3	33 *	0	5	6	22	28

* Eight weaknesses were reported as closed in Q2 in error, but six of them were actually closed in Q3, so they should not be counted at the start of the quarter since they were already counted as closed in the previous quarter.

Table C-2. System Level POA&Ms Statistics

Quarter	# At Start of Quarter	# New	# Completed	# Ongoing	# Delayed	# For Start of Next Quarter
Q1	172	32	4	56	144	200
Q2	200	10	10	40	160	200
Q3	201 **	1	37	37	128	165

** Three weaknesses were reported as closed in Q2 in error, but two of them were actually closed in Q3, so they should not be counted at the start of the quarter since they were already counted as closed in the previous quarter.

Table C-3 summarizes the total number of weaknesses included in the FY 2007 POA&Ms, the total number of corrective actions actually completed, the total number of corrective actions that are still ongoing, and the number of corrective actions whose completion has been delayed. The statistics are based on Tables C-1 and C-2 above.

Table C-3. Summary of FY 2007 POA&Ms Through the 3rd Quarter

	Total # Weaknesses	Total # Completed	Total # Ongoing	Total # Delayed	% Completed
Program Level	40	14	6	22	35%
System Level	215	51	37	128	23.7%

In the agency's 3rd Quarter FY 2007 FISMA update to OMB, the agency reported that up to 20 percent of the weaknesses for various systems were closed this quarter. This is misleading because:

- One of the three weaknesses reported as closed for a system was reported as closed in a previous quarter.
- Five of the eight weaknesses reported as closed for a system were related to updates to the system's contingency plan. The five weaknesses were noted on the POA&M as duplicates of another weakness and were closed. The updates to the contingency plan were eventually completed, but not until after the five weaknesses had been reported as closed.
- All nine of the weaknesses reported as closed for a legacy system were closed because a decision was made at the agency level not to continue with the certification and accreditation of the system, which is undergoing modernization. Upon issuing the system's IATO, the DAA decided not to require the system owner to continue development of the contingency plan and security plan. The nine weaknesses were closed as a result of this decision and not because the corrective actions to address the weaknesses had been completed. The contingency plan for this system was eventually updated and tested, but not until after the nine weaknesses had been reported as closed.
- Four of the five weaknesses reported as closed for a system were reported as closed in previous quarters.

Appendix D. FY 2007 OMB FISMA REPORTING TEMPLATE FOR IGs

This appendix contains the FY 2007 OMB FISMA Reporting Template for IGs (referred to by OMB as Section C) and the additional narrative that will be included in the agency's FISMA submission to OMB.

Section C - Inspector General: Questions 1 and 2

Agency Name: **Nuclear Regulatory Commission** **Submission date:** **25-Sep-07**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
NRC	High	4	0	0	0	4	0	1	25%	4	100%	0	0%
	Moderate	11	1	4	0	15	1	5	33%	13	87%	7	47%
	Low	0	0	1	0	1	0	1	100%	1	100%	0	0%
	Not Categorized	15	0	6	0	21	0	0	0%	18	86%	0	0%
	Sub-total	**30**	**1**	**11**	**0**	**41**	**1**	**7**	17%	**36**	88%	**7**	17%
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Component/Bureau	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**4**	**0**	**0**	**0**	**4**	**0**	**1**	25%	**4**	100%	**0**	0%
	Moderate	**11**	**1**	**4**	**0**	**15**	**1**	**5**	33%	**13**	87%	**7**	47%
	Low	**0**	**0**	**1**	**0**	**1**	**0**	**1**	100%	**1**	100%	**0**	0%
	Not Categorized	**15**	**0**	**6**	**0**	**21**	**0**	**0**	0%	**18**	86%	**0**	0%
	Total	**30**	**1**	**11**	**0**	**41**	**1**	**7**	17%	**36**	88%	**7**	17%

Section C - Inspector General: Question 3

Agency Name:	**Nuclear Regulatory Commission**	
	Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory	
3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Mostly (81-95% of the time)
3.b.	**The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 81-95% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes

3.f. **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI)	Agency or Contractor system?

Number of known systems missing from inventory:	

Section C - Inspector General: Questions 4 and 5

Agency Name: Nuclear Regulatory Commission

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:

- **Rarely- for example, approximately 0-50% of the time**
- **Sometimes- for example, approximately 51-70% of the time**
- **Frequently- for example, approximately 71-80% of the time**
- **Mostly- for example, approximately 81-95% of the time**
- **Almost Always- for example, approximately 96-100% of the time**

4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Almost Always (96-100% of the time)
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Almost Always (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Almost Always (96-100% of the time)
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always (96-100% of the time)

POA&M process comments: NRC has two primary tools for tracking IT security weaknesses. At a high level, NRC uses the POA&Ms required by OMB to track (1) corrective actions from the OIG annual independent evaluation, (2) corrective actions from the agency's annual review, and (3) recurring FISMA and IT security action items such as annual self-assessments and annual contingency plan testing. The POA&Ms may also include corrective actions resulting from other security studies conducted by or on behalf of NRC. The more specific corrective actions associated with the certification and accreditation process (e.g., corrective actions resulting from risk assessments and security test and evaluation) are tracked in Rational ClearQuest as change requests using the project management methodology process for change management.

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Failing	
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	
		Security awareness training	
		Configurations/patching	X
		Other: Risk Asssessment	X

C&A process comments: Indicent handling and security awareness training were evaluated at the agency level. For more details on the agency's certification and accreditation process, see attached narrative, pages 4 and 5.

Section C - Inspector General: Questions 6 and 7

Agency Name:	**Nuclear Regulatory Commission**	
	Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process	
6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Excellent
	Comments:	
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	**Excellent**
	Comments:	
	Question 7: Configuration Management	
7.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
	Comments:	
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **Response categories:** - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Rarely (0-50% of the time)

Section C - Inspector General: Questions 8, 9, 10 and 11		
Agency Name: Nuclear Regulatory Commission		
Question 8: Incident Reporting		
Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.		
8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes
	Comments:	
Question 9: Security Awareness Training		
Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? **Response Categories:** **- Rarely- or approximately 0-50% of employees** **- Sometimes- or approximately 51-70% of employees** **- Frequently- or approximately 71-80% of employees** **- Mostly- or approximately 81-95% of employees** **- Almost Always- or approximately 96-100% of employees**		Almost Always (96-100% of employees)
Question 10: Peer-to-Peer File Sharing		
Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.		**Yes**
Question 11: E-Authentication Risk Assessments		
The agency has completed system e-authentication risk assessments. Yes or No.		**No**
While OMB M-04-04 only requires e-authentication risk assessments for e-Government systems, NRC requires e-authentication risk assessments for all agency systems that require security categorizations. The e-authentication risk assessment is conducted during the security categorization of a system. The agency has completed all e-authentication risk assessments required under OMB M-04-04; however, the agency has not completed e-authentication risk assessments for all agency systems in accordance with its own policy.		

The following supplemental information is provided in support of the FY 2007 Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) Reporting Template for Inspectors General for the Nuclear Regulatory Commission (NRC). The independent evaluation of NRC's implementation of FISMA for FY 2007 was conducted by Richard S. Carson and Associates, Inc. (Carson Associates) on the behalf of the NRC Office of the Inspector General (OIG).

Question 1a. NRC has a total of 30[25] operational systems that fall under FISMA reporting requirements.[26] Of the 30, 17 are general support systems, and 13 are major applications. As required by FISMA, Carson Associates selected a subset of NRC systems for evaluation during the FY 2007 FISMA independent evaluation. However, only one of the three systems that were selected had a current certification and accreditation. While an additional system completed certification and accreditation in July 2007, it was after the cutoff date established at the entrance conference, and was therefore not considered for evaluation. As there were no other systems

[25] The agency reports 31 operational systems. The OIG disagrees with the agency that an OIG system is a major application. It has been categorized as a listed system since it began operations in 2004. This designation is presently under a detailed review. Therefore, the metrics submitted by the OIG reflect a total of 30 operational systems.

[26] NRC also has a number of major applications and general support systems currently in development. For FISMA reporting purposes, only operational systems are considered.

with a current certification and accreditation to consider for evaluation, Carson Associates evaluated only one agency system for the FY 2007 FISMA independent evaluation.

Question 1.b. NRC has a total of 11 systems operated by a contractor or other organization on behalf of the agency (8 major applications and 3 general support systems). Of the 11, 6 are operated by other Federal agencies, 2 are operated by federally funded research and development centers, and 3 are operated by private contractors. NRC is responsible for direct oversight for four of these systems. Oversight of the remaining seven systems is the responsibility of the Federal agency operating the system. Therefore, the OIGs of those agencies would be responsible for evaluating those systems.

As required by FISMA, Carson Associates selected a subset of the contractor systems for which NRC is responsible for direct oversight for evaluation during the FY 2007 FISMA independent evaluation. However, the system selected did not have a current certification and accreditation, and none of the other contractor systems for which NRC is responsible for direct oversight had a current certification and accreditation. Therefore, Carson Associates did not evaluate any contractor systems for the FY 2007 FISMA independent evaluation.

Question 2. The metrics in Question 2 represent the status for all NRC systems, not just the subset that was chosen for evaluation in FY 2007.

Question 2.a. Only two agency systems are certified and accredited, and only five systems operated by a contractor or other organization on behalf of the agency are certified and accredited. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements and that other contractor systems are certified and accredited.

In accordance with OMB requirements, it constitutes a ***significant deficiency*** that only 2 of the 30 operational NRC information systems have a current certification and accreditation and only 5 of the 11 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation.

Subsequent to the completion of fieldwork, the agency reported that two additional agency systems have also been certified and are currently under review by the agency's designated approving authority for consideration of an ATO.

Question 2.b. NRC meets the FISMA requirement to test and evaluate the security controls of agency information system on an annual basis by performing annual self-assessments of the security controls of all agency and contractor systems. NRC performed self-assessments of the security controls for 28 of the agency's 30 operational systems. The agency chose not to perform a self-assessment of the OIG system discussed earlier, as that system's status as a major application is still under determination. As the other two agency operational systems were just certified and accredited in FY 2007, the agency did not perform an additional self-assessment of those systems as permitted by OMB and National Institute of Standards and Technology (NIST) guidance. The agency also included the physical and environmental controls of the four NRC regional offices and the NRC Technical Training Center in one self-assessment.

NRC is required to perform self-assessments only on those contractor systems for which it has direct oversight. Self-assessments for the remaining contractor systems are the responsibility of the Federal agencies that operate those systems. NRC performed a self-assessment of one of the four contractor systems for which it has direct oversight. As two of the four contractor systems for which NRC has direct oversight are considered to be sub-components of the NRC LAN/WAN, only the physical and environmental controls and the personnel security controls were evaluated for these systems. The results were incorporated into the self-assessment for one of the agency's general support systems. The fourth contactor system for which the agency has direct oversight was expected to be certified and accredited in FY 2007, so the agency did not conduct a separate self-assessment for this system. However, the certification and accreditation was not expected to be completed prior to the submission of this report, so it was not originally included in the total number of contractor systems for which security controls have been tested and evaluated in the past year. Subsequent to the completion of fieldwork, the agency completed certification and accreditation of this system, and the system was granted an ATO.

For the seven contractor systems that are operated by other Federal agencies, NRC's policy is to confirm with the owner agencies that annual security control testing and evaluation has been completed. As two of the Federal contractor systems were just certified and accredited in FY 2007, these two systems were included in the total number of contractor systems for which security controls have been tested and evaluated. The agency has not obtained confirmation from the owner agencies of the other five contractor systems operated by other Federal agencies that annual security control testing and evaluation has been completed. Subsequent to the completion of fieldwork, the agency provided a certification memorandum for one of the Federal contractor systems that indicates security control testing and evaluation for the system was completed in FY 2007. However, the agency could not demonstrate that this system has been accredited (and therefore, that the designated approving authority for that system approved the testing and evaluation). Therefore, it was not included in the total number of contractor systems for which security controls have been tested and evaluated in the past year.

The agency did not use NIST Special Publication (SP) 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, for the annual assessment of security control effectiveness, but instead used the methodology described in NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*. Carson Associates also found that self-assessments were not always based on an approved security categorization and that self-assessments contained errors and inconsistencies.

Question 2.c. Only five agency systems and one contractor system has had its contingency plan tested in the past year. Subsequent to the completion of fieldwork, the agency provided documentation demonstrating that contingency plan testing was conducted for another contractor system; however, the agency has not yet received the test results report. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements (including annual contingency plan testing).

In accordance with OMB requirements, the fact that the agency has failed to conduct annual contingency plan testing for all systems for the past 3 years constitutes a ***significant deficiency***.

Question 3.a. NRC presumes that the Federal agencies that operate 7 of the 11 contractor systems are also following FISMA and guidelines from NIST. The agency has been working with the offices to assist in acquiring the required documentation for systems provided by other Federal agencies. However, according to the agency, some of the other Federal agencies have been unwilling to provide documentation that demonstrates they meet FISMA requirements. The other Federal agencies have also been unwilling to share copies of their annual self-assessments or results from their annual contingency plan testing. The OIG stated that a memorandum from the Federal agencies stating that annual self-assessments and annual contingency plan testing have been completed would be sufficient to meet the intent of the recommendations from the FY 2005 FISMA independent evaluation regarding this finding. The agency is currently working towards obtaining such memoranda. As of September 1, 2007, the agency had received certification and accreditation memoranda for only four of the seven systems provided by or operated by other Federal agencies. Due to the current focus on the certification and accreditation phase of systems and scarcity of resources, the anticipated completion date to receive the rest of the required documentation for systems provided by or operated by other Federal agencies is December 31, 2007.

Question 3.b. While FISMA requires agencies to maintain an inventory only of major information systems (major applications and general support systems), NRC also tracks two other system types in its inventories – listed[27] and other.[28] To address findings from the FY 2005 FISMA independent evaluation regarding the agency's inventory, OIS developed a new centralized system for tracking NRC information systems. Data from various databases were compared, and any differences were resolved. The new system was then updated with data from biannual data calls, starting in September 2006. The new system continues to be updated with subsequent data calls. The agency also developed several procedures and guides to assist NRC offices with the biannual data call and to assist the agency in maintaining the inventory data in the new system.

Carson Associates found small discrepancies between the inventory of major applications, general support systems, and contractor systems reported in the metrics to OMB, and the actual contents of the agency's new inventory system. The agency has been made aware of these minor discrepancies and is working to correct them. Carson Associates also found that the agency is still in the process of populating the new inventory system with information on interfaces between systems. The agency is also still working to complete one recommendation from the FY 2006 FISMA independent evaluation regarding the classification of the agency's Network Continuity of Operations (COOP) system. This system was categorized as a listed system, when it should have been categorized as a general support system. The agency has incorporated the components of the COOP system into existing infrastructure general support systems, and is no longer tracking the COOP system as an individual system. The agency has updated the security

[27] Listed systems are computerized information systems or applications that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which are not a major application or general support system when viewed from an agency perspective. Sensitive data may include individual Privacy Act information, law enforcement sensitive information, sensitive contractual and financial information, safeguards, and classified information.

[28] Other systems are NRC systems that do not require additional security protections and are adequately protected by the security provided by the NRC local area network/wide area network.

categorization documents for four general support systems to incorporate the appropriate COOP components, but they have not all been approved by the Senior Agency Information Security Officer.

Question 4. While the agency's POA&M process is adequate, the agency has made minimal progress in correcting weaknesses reported on its POA&Ms. The agency has corrected 35 percent of its program level weaknesses, and 23.7 percent of its system level weaknesses. This is only a slight improvement over FY 2006. The majority of delays have been caused by delays in completing certifications and accreditations. Carson Associates also found that the quality of the agency's POA&Ms needs improvement.

Question 5.a. To correct weaknesses identified by the FY 2005 and FY 2006 FISMA independent evaluations by the NRC OIG, and to address findings from the agency's own evaluation, the agency has refocused its information system security program. Under the refocused program, the agency proposed performing certification and accreditation of systems that are a high priority from a mission perspective and others that potentially pose a higher security risk (e.g., agency systems that communicate with systems outside the NRC network). The first certification and accreditation schedule under the refocused program was issued in February 2006. This schedule has changed several times since February 2006.

The first phase of the refocused program included the development of a new certification and accreditation process, which has been finalized. The agency has finalized the templates for all certification and accreditation documents as well as instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology. One of the agency's operational major applications was chosen to "pilot" the new process and documentation standards, in part, to ensure the new process is repeatable.

Even with the new certification and accreditation process, the refocused information system security program, and the award of a multi-year, multi-million dollar contract to provide the agency with consolidated information system security services, the agency has completed certification and accreditation of only two agency systems and one contractor system for which the agency has direct oversight in the past 2 years. In the meantime, the certifications and accreditations for all of the agency's remaining 28 operational systems have expired.

As stated previously, it constitutes a ***significant deficiency*** that only 2 of the 30 operational NRC information systems have a current certification and accreditation and only 5 of the 11 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation.

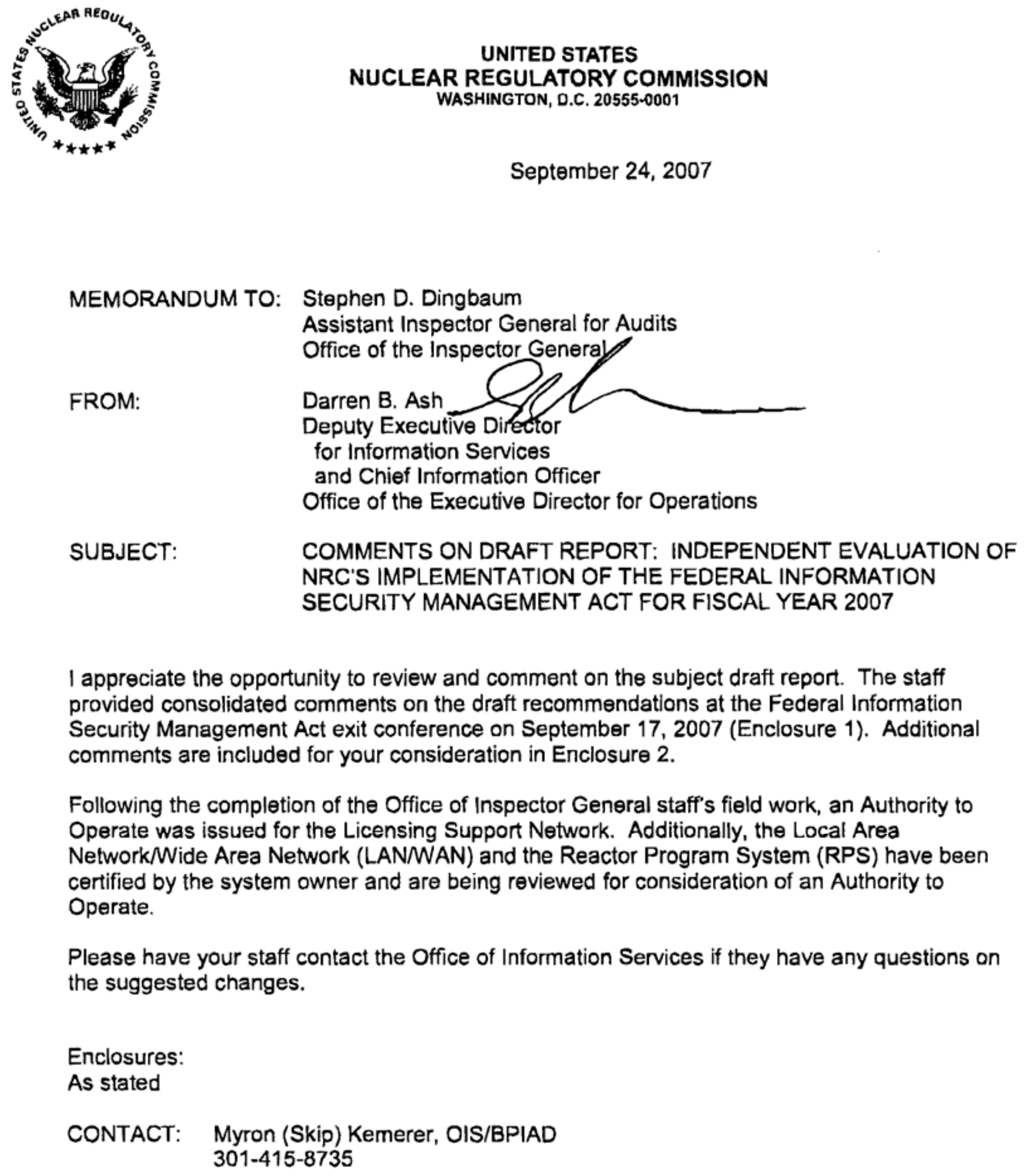
We rated the overall quality of the agency's certification and accreditation process as failing because the agency has completed the certification and accreditation of only two agency systems and one contractor system for which the agency has direct oversight in the past 2 years. The failing rating does not necessarily reflect the actual quality of the process itself. Carson Associates could not perform a complete evaluation of the agency's new certification and accreditation process, as only two systems had completed certification and accreditation under the new process at the time of our evaluation. Based on the certification and accreditation documents we did review, we found that the agency's certification and accreditation process is inconsistent with NIST guidance.

Question 9. NRC ensures all employees and contractors receive security awareness and training. However, the agency still has not met the requirement to provide specialized training for employees with significant security responsibilities as described in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Mode*. The agency is still working with NRC offices to identify employees and contractors with significant IT security responsibilities. The agency is also still developing procedures for ensuring staff with significant IT security responsibilities are identified and receive security awareness training and that the individual and associated training are properly documented and readily identifiable.

Question 11. While OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, only requires e-authentication risk assessments for e-Government systems, NRC requires e-authentication risk assessments for all agency systems that require security categorizations. The e-authentication risk assessment is conducted during the security categorization of a system. The agency has completed all e-authentication risk assessments required under OMB M-04-04; however, the agency has not completed e-authentication risk assessments for all agency systems in accordance with its own policy. Only 15 of the 30 operational NRC information systems have completed e-authentication risk assessments. Only 5 of the 11 contractor systems have completed e-authentication risk assessments. According to the agency, the target date for completing all e-authentication risk assessments was July 30, 2007. This target date was not met.

[Page intentionally left blank]

Appendix E. MEMORANDUM TRANSMITTING AGENCY RESPONSE



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

September 24, 2007

MEMORANDUM TO: Stephen D. Dingbaum
Assistant Inspector General for Audits
Office of the Inspector General

FROM: Darren B. Ash
Deputy Executive Director
for Information Services
and Chief Information Officer
Office of the Executive Director for Operations

SUBJECT: COMMENTS ON DRAFT REPORT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2007

I appreciate the opportunity to review and comment on the subject draft report. The staff provided consolidated comments on the draft recommendations at the Federal Information Security Management Act exit conference on September 17, 2007 (Enclosure 1). Additional comments are included for your consideration in Enclosure 2.

Following the completion of the Office of Inspector General staff's field work, an Authority to Operate was issued for the Licensing Support Network. Additionally, the Local Area Network/Wide Area Network (LAN/WAN) and the Reactor Program System (RPS) have been certified by the system owner and are being reviewed for consideration of an Authority to Operate.

Please have your staff contact the Office of Information Services if they have any questions on the suggested changes.

Enclosures:
As stated

CONTACT: Myron (Skip) Kemerer, OIS/BPIAD
301-415-8735

[Page intentionally left blank]

Appendix F. FORMAL AGENCY COMMENTS AND DETAILED OIG ANALYSIS OF AGENCY COMMENTS

At an exit conference with the agency held on September 17, 2007, the agency provided informal written comments and generally agreed with the report recommendations. The NRC Chief Information Officer provided a formal response to this report on September 24, 2007. Appendix E contains the Chief Information Officer's transmittal letter. This appendix contains the agency's formal comments along with OIG's analysis and response to those comments. NRC's comments are presented in their entirety and appear in italics, followed by the OIG analysis of the comments. This final report incorporates revisions made, where appropriate, in response to the agency's comments.

General Comments

Credit is not given in the "Results in Brief" section for the positive finding with respect to how the agency is managing Privacy and PII information. We request this section include these positive results.

The report was modified to note the agency's progress in managing Privacy and PII information.

Comments on Recommendations

1. *Staff believes Security Categorizations are correct based on the information in their systems. Staff is not aware of a requirement that the information type listed in the Security Categorization has to match the Exhibit 53.*

The report was not modified. While it is true that there is no requirement that the information type listed in the Security Categorization has to match the Exhibit 53, it is implied by the process described in NIST SP 800-60 Volume I. The methodology described in NIST SP 800-60 Volume I includes:

- Identifying the fundamental business areas (management and support) or mission areas (mission-based) supported by the system under review.
- Identifying for each business or mission area the areas of operations or lines of business that describe the purpose of the system in functional terms.
- Identifying the sub-functions necessary to carry out each area of operation or line of business.
- Selecting the basic information types associated with the identified sub-functions.

The Exhibit 53 is the primary source for the business area, line of business, sub-function, and information type.

> *Additionally, staff does not believe any system has an inappropriate categorization because the information type in the Security Categorization (Sec Cat) does not match the Exhibit 53.*

The report was not modified. While it may be true that the overall system categorizations themselves are appropriate (i.e., the systems are correctly identified as low-, moderate-, or high-impact systems), it is still important to correctly identify the information types that lead to that security categorization. NIST will be updating NIST SP 800-60 in the next few months. The correct information types need to be identified so that the agency can review the modifications NIST makes to those information types in NIST SP 800-60 to see if the changes have any impact on the security categorizations.

2. *NRC does not perform Sec Cats on other federal agencies' systems, but performs Sec Cats on the NRC information that is being processed on those other agencies' systems. This is the only documentation NRC has to understand what NRC information is being placed on those systems. NRC uses the results of the Sec Cat performed on our information to ensure the security level of the hosting system meets NRC's requirements. We request that this discussion leading up to the recommendation be deleted.*

The report was modified and the discussion of performing security categorizations of other Federal agencies' systems was removed as a cause for Finding B. However, it should be noted that while the agency's explanation for why they performed security categorizations of other Federal agencies' systems is reasonable, this rationale is not clearly reflected in the security categorizations. The security categorizations that NRC performed on the other Federal agencies' systems give no indication that the focus was just on the NRC information that is being processed on that other agencies' systems, or that the focus was just on the interface with the other agencies' systems.

3. *Staff believes the self assessments were consistent with the guidance in the Fiscal Year 2006 Federal Information Security Management Act reporting guideline (OMB-M-06-20) which states that National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a, Guide for Assessing the Security Controls in Federal Information Systems, is to be used for the assessment. NRC used the NIST SP 800-53a criteria in completing the self assessments. NIST SP 800-53a provides a short sample reporting template for illustrative purposes that is geared towards Security Test and Evaluation. An agency may use choose to use another format (page 373). NRC used the NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, format, which also agrees with the agency assessment reporting format as shown in NIST SP 800-100, Information Security Handbook: A Guide for Managers. While NRC used the NIST SP 800-26 reporting format, we changed all of the data elements to capture all of the security controls listed in NIST SP 800-53 Rev. 1, Recommended Security Controls for Federal Information Systems, and we evaluated our controls against NIST SP 800-53a criteria. We believe that a review of the controls used in the self assessments will show that the NIST SP 800-53a controls were the basis for the self assessments.*

The report was not modified. We disagree with the statement that the agency used NIST 800-53A criteria in completing the self assessments. There is almost no mention of using SP 800-53A in any of the documentation provided by the agency regarding self-assessments. The task order issued to perform the self-assessments stated that the assessments should be consistent with draft NIST SP 800-26 Revision 1 (including Appendix A System Questionnaire) and NIST SP

800-53 Revision 1. Draft NIST SP 800-26 Revision 1 was pulled from the NIST Web site and is not even considered a draft any more. The only SP 800-26 Revision 1 document still on the NIST Web site is the questionnaire from the original SP 800-26 with mappings to the controls in SP 800-53. The task order mentions the use of SP 800-53A, but only once. The task order primarily focuses on the use of SP 800-26. The task order also mentions the NRC System ST&E plan template, which does not seem to have been used at all during the self-assessments. The agency also provided a self-assessment overview document. In the section on the self-assessment process, the methodology the agency planned on using was described as the "self-assessment approach of measuring progress by levels of effectiveness … continues to follow the NIST SP 800-26 guidance." This document makes no mention of using SP 800-53A, and the process described in this document is the methodology described in SP 800-26. It is not the SP 800-53A methodology. The actual self-assessments also make no mention of using SP 800-53A. They state that the self-assessments were based on NIST SP-800-26 dated April 2005. It is also not the case that no other format was specified, other than the sample reporting template in SP 800-53A. As stated in this report, NIST issued a memorandum for the record in February 2007 (updated in May 2007), that included as an attachment a security controls assessment form, which replaces the form contained in NIST SP 800-26, and provides a standard methodology for capturing the results of system-level security control assessments. The form from SP 800-100 that the agency references in their comments is for assessing an information security program, and it not intended to be used to assess an individual system. While it is true that controls used in the self assessments are the controls found in NIST SP 800-53A, the issue is not with the controls that were evaluated, but with the methodology used to evaluate them. The agency has not provided any documentation that demonstrates that the methodology described in SP 800-53A was used to conduct the self-assessments.

4. *Agree. Some were based on revised Sec Cats that have been submitted but not approved to date.*

No changes to the report were necessary.

5. *Agree, if language concerning "free from errors and inconsistencies" is dropped.*

The recommendation was modified as suggested.

6. *Agree, written comments will provide some updates.*

No changes to the report were necessary.

7. *Agree. Staff has been requesting copies as Authorities to Operate are being worked.*

Recommendation 7 was modified to incorporate the intent of recommendations 8 and 9. Recommendations 8 and 9 were removed from the report.

8. *Agree, if the language is revised to recommend "maintaining evidence that self assessments were completed" vs. having copies of self assessments. Agencies will not provide copies of self assessments.*

Recommendation 7 was modified to incorporate the intent of recommendations 8 and 9. Recommendations 8 and 9 were removed from the report.

9. *Agree, if the language is revised to recommend "maintaining evidence that contingency plan tests were completed" vs. having copies of self assessments. Agencies will not provide copies of test results.*

Recommendation 7 was modified to incorporate the intent of recommendations 8 and 9. Recommendations 8 and 9 were removed from the report.

10. *Agree. This was addressed in a recent update to the previous report.*

No changes to the report were necessary.

11. *Addressed in an update to the previous report. Under the current approach, there is no system called Network Continuity of Operations.*

The recommendation was modified to reflect the fact that there is no system called Network Continuity of Operations, but that the security categorizations of the general support systems into which the Network Continuity of Operations components have been incorporated have not all been updated.

12. *Agree.*

No changes to the report were necessary.

13. *Agree, if language concerning "free from errors and inconsistencies" is dropped.*

The recommendation was modified as suggested.

14. *Agree.*

No changes to the report were necessary.

15. *While we agree with the recommendation, we believe the current approach is consistent with the resources available. The most important controls were tested.*

No changes to the report were necessary.

16. *Agree. Procedures are in development and contracts are being developed to provide the training, starting with system administrators and system security officers.*

No changes to the report were necessary.

17. *Please change the language to read "Review and update the remaining two e-Authentication risk assessments as specified in recommendation 8 of OIG-05-A-21 to correct inaccuracies and inconsistencies with FIPS 199 security categorizations."*

Recommendation 17 was removed from the report, and incorporated into recommendation 18 (which is now recommendation 15).

18. *Agree.*

No changes to the report were necessary.

<u>Additional Comments</u>

1. *Line 320. Status of Security Plan Documentation*

   Notes that the agency updated security plans for 5 of the agency's 30 operational systems. The list did not include the Licensing Support Network (LSN). The LSN Security Plan is in ADAMS (ML072340242) and its revision history indicates an Initial Release existed at the time of the evaluation:

Date	*Version*	*Description*	*Author*
8/17/2007	*1.1*	*Updated to reflect findings from Security Test and Evaluation conducted by Atomic Safety and Licensing Board Panel (ASLBP) and AT&T Government Solutions*	*MAR, Incorporated*
6/11 /2007	*1.0*	*Initial Release*	*MAR, Incorporated*

   Accordingly, we believe that the LSN should have been included in the list for which new/updated Security Plans were developed during Fiscal Year (FY) 2007. Please include this in your numbers.

The report was modified as suggested. However, it should be noted that the security plan was not provided by the cutoff date established at the entrance conference. While the update may have occurred August 17, 2007, the document was not placed in ADAMS until August 24, 2007, which was after the cutoff date established at the entrance conference. The agency also did not include this security plan in metrics it provided to the OIG with the 4th Quarter FY 2007 POA&M submission.

2. *Line 341. We suggest that the sentence be amended (in italics) to read "Annual contingency plan testing is still not being performed for all systems." On page 22, beginning on line 863, it is indicated that contingency plan testing has been conducted for some systems.*

The report was modified as suggested.

3. *Line 471. Security Categorization for the LSN Exhibit 53 Issue.*

Page 9, Finding A
Identifies the LSN as having a security categorization that did not reflect the primary business area, primary line of business, and/or primary sub-function of those systems as indicated on the Exhibit 53.

Agreed as factual, however, there is no requirement for reconciliation between the Sec Cat and the Exhibit 300 and we believe this finding should be deleted.

The report was modified to remove LSN as an example of a security categorization that is inconsistent with the Exhibit 53. The agency's rationale (item 4 below) is sufficient to explain the inconsistency. However, the overall finding was not deleted as suggested. See our response to the agency's comments on recommendation #1.

4. *Line 501. National Institute of Standards and Technology (NIST) Information Type Issue.*

Page 10, Finding A
Asserts that the Information Type in the Security Categorization does not even reflect the actual mission of the system.

Since June 2004, ASLBP, the Office of Information Services (OIS), and the contractor teams working on LSN Certification and Accreditation (C&A) efforts have struggled with the failure of NIST to address portal and text indexing environments in NIST 800-60 and the intermittent spidering and data extraction that is a different paradigm than peer-to-peer data sharing as described in SP 800-47.

The description in NIST 800-60 at page 229 is as follows (with emphasis added):

> *"D.22.4 Information Infrastructure Management Information Type Information Infrastructure Management involves the management and stewardship of a type of information by the Federal Government and/or the creation of physical communication infrastructures on behalf of the public in order to facilitate communication. This includes the management of large amounts of information (e.g., environmental and weather data, criminal records, etc.), the creation of information and data standards relating to a specific type of information (patient records), and the creation and management of physical communication infrastructures (networks) on behalf of the public."*

The recommended provisional security categorization for the information infrastructure maintenance information type is as follows: Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}.

The information content in the LSN system is almost a precise match for this description. Excluding help pages, the LSN is a network comprised of: (1) a Commercial Off-the-Shelf (COTS) full text search engine (2), "Spidering" software, and (3) indexes.

> *The role of the LSN Administrator as defined in 10 CFR Part 2, Subpart J is the role of a manager and independent steward. The LSN is a network of 14 interconnected computer systems, only two of which are federal. The system is publicly accessible, without access controls, via the internet. The user community is comprised of non-government and government users. It facilitates the identification, search and retrieval of information. It contains a large amount of information. The system mission is outlined in 10 CFR Part 2, Subpart J and the data content specifically represents and precisely fulfills the requirement at 10 CFR § 2.1011 (b)(2)(i). The system follows information and data standards defined by NRC at 10 CFR § 2.1011 (b)(2)(ii) et seq.*
>
> *The specific type of information to be included, as well as information to be excluded, is described in 10 CFR § 2.1003 and § 2.1005. NRC created and manages the central indexing system, web hosting, and telecommunications infrastructure that enables the system.*
>
> *The information type described in NIST 800-60 as quoted above, objectively read, matches the mission and operation of the LSN. It is acknowledged that it is outside the construct of "public goods construction" but ASLBP did not craft the taxonomic structure of the NIST guidance or have an opportunity to bring this particular shortcoming, or the lack of adequate coverage for portals and web indexes in general, to their attention. Conversely, it is arguable that classifying the information type per NIST 800-60, Section D.17.1 Judicial Hearings Information Type[29] is inappropriate because document discovery is typically transacted between parties and external to the agency's adjudicatory process.*
>
> *Finally, the Independent Evaluation recommends using the "permits and licensing information type under the regulatory and compliance enforcement line of business." ASLBP agrees to explore adding this to the information type discussion in the LSN system documentation, but notes that per the discussion in NIST 800-60 for the Permits and Licensing Information Type,[30] the recommended security categorization would continue to be "Security Category = {(confidentiality, Low), (integrity, Low), (availability, Low)}." We believe that the narrative regarding the LSN's current information type categorization not reflecting the risk impact to the agency should be removed as a finding.*

The report was modified to remove LSN as an example of a security categorization that is inconsistent with the Exhibit 53, including the discussion of alternative information types for that system. The agency's rationale is sufficient to explain their choices in determining the system's information type. However, the overall finding was not deleted as suggested. See our response to the agency's comments on recommendation #1.

5. *Lines 563-570. This seems to contradict the earlier sentences (541-553) "Categorize all NRC information systems, including systems operated by a contractor or other organization on behalf of the agency, in accordance with Federal Information Processing Standards (FIPS) 199." If this sentence means to have up-to-date security documentation from the*

[29] Judicial hearings include activities associated with conducting a hearing in a court of law to settle a dispute.

[30] Permits and Licensing involves activities associated with granting, revoking, and the overall management of the documented authority necessary to perform a regulated task or function.

systems operated by other organizations on behalf of the agency, it should be more clear and concise in meaning.

The report was modified to remove the discussion regarding performing security categorizations for systems that are not major applications or general support systems, or are operated by other Federal agencies. Minor modifications were made to the recommendation to make it clear that the agency should complete the security categorization of all their major applications and general support systems.

6. *Lines 621-622. Please examine the sentence as the phrase "..., but less than annually" should probably read "..., but no less than annually" as it does in line 675 on page 16.*

The report was modified to read "but not less than annually."

7. *Lines 653-662. The Office of Administration (ADM) has received the annual security control testing and evaluation for FPDS-NG. The document is dated May 24, 2007.*

The report was not modified. The agency provided a certification memorandum for FPDS-NG that supports the statement that security control testing and evaluation for FPDS-NG was completed in FY 2007. However, the agency could not demonstrate that this system has been accredited (and therefore, that the designated approving authority for that system approved the testing and evaluation). Therefore, it was not included in the total number of contractor systems for which security controls have been tested and evaluated in the past year.

8. *Lines 711-716. The bullets do not fully describe that "for 2 operational systems, the FEES and HRMS, additional evaluations were conducted to validate that controls were implemented and to assess compensating controls, even though policies and procedures may not have been fully in place." We request this sentence be updated in the report.*

The report was not modified. We acknowledge that the self-assessments for the two systems noted above include descriptions of controls in place in the "Comments" column, and that they also include, where needed, a discussion of compensating controls. However, there is no evidence that additional evaluations were conducted to obtain this information. The presence of the additional information in the self-assessments does not clearly demonstrate that additional evaluations were conducted. The self-assessments only mention document reviews and interviews as methods used to conduct the self-assessments.

9. *Lines 727 and 728. We do not agree with the sentence "For example, if a control had policies, but no procedures, then the implementation of that control was never evaluated, even if the control was actually implemented." We suggest adding the following (in italics): "For example, except for 2 systems (FEES and HRMS), if a control had policies…"*

The report was modified to state "then the implementation of that control was, in most cases, never evaluated."

10. *Lines 783-792. Integrated Personnel Security System (IPSS) discussions occurred between ADM and OIS and it was determined that the system had originally been listed as a high-impact security control baseline and that it should be a moderate-impact security control baseline. This was discussed during the self-assessment interview, but there was no area in the self-assessment document that requested discussion for the change. The IPSS Security Categorization has gone forward from ADM to OIS for review and approval.*

The report was not modified, but the agency's comment is noted.

11. *Lines 865 and 866. Please amend (in italics) the sentence to read "2 (FFS and FPPS) of the agency's contractor systems, had their contingency plans tested in FY 2007." A contingency plan test was conducted for the FPPS on August 15, 2007, which may have been after the field work was completed for this evaluation. We have requested but have not yet received the test results report; however, we do have email traffic and contact names available as evidence of the testing, which we can provide. Please also update the table on page 69 to reflect this date, and the scheduled date for August 2008.*

The metrics were modified to reflect annual contingency plan testing for FPPS. The agency provided documentation that demonstrates contingency plan testing was conducted for FPPS in August 2007. It should be noted that our criteria for including contingency plan testing in the metrics is that not only must the testing have occurred before the cutoff date established at the entrance conference, but the test report results must also have been submitted to and approved by the agency prior to or on the cutoff date. We do not count contingency plan tests that are not supported by a test report that has been approved by the agency. It should also be noted that the agency did not count annual security control testing for FPPS in the metrics it provided to the OIG with the 4th Quarter FY 2007 POA&M submission.

12. *Lines 887-907. IPSS has not had a planned contingency plan test done since 2004. However, the contingency plan has been tested in actual operations six times since that period due to system outages for upgrades or maintenance. In each case implementation of the contingency plan was successful and no deficiencies were identified. We request this information be added to the report or the finding dropped.*

The report was not modified as the agency has not provided any evidence to support the statement that the contingency plan has been tested in actual operations due to system outages for upgrades or maintenance. It should be noted that testing of a contingency plan in actual operations is an accepted form of contingency plan testing and can be documented in a contingency plan test report. The testing of the contingency plan in actual operations would have been counted if it had been documented.

13. *Line 915. If bracketed items are to be carried over to the final report then "...[CNRWA, …" should be "...[CNWRA,..."*

All system names in brackets were removed from the discussion draft before the report was submitted as a final.

14. *Line 918. Contingency Plan Testing for Low Risk Systems. Pages 23, 24, Finding G identifies the LSN as one of the 10 systems that did not complete contingency plan testing.*

    ASLBP was advised by OIS and the contractors supporting the development of the C&A package for the LSN that annual contingency plan testing is not required for systems with "Low-Low-Low" risk assessments, whereas the Independent Evaluation asserts that this is a "requirement." Page 3 of Annex 1 Low Impact Baseline to 800-53 specifies for control family Contingency Planning, (CP-4) Contingency Plan Testing and Exercises "not selected." Accordingly we request this finding be removed.

The report was not modified. While it is true that NIST SP 800-53 Revision 1 does not require contingency plan testing (control CP-4) for low-impact systems, the agency requires contingency plan testing for all major applications and general support systems. This requirement can be found in several documents including:

- MD and Handbook 12.5, Table 3-1, page 35
- OIS-9000D-004 Revision 0, *Ensure Contingency Plans are Tested Annually for Major Applications (MA) and General Support Systems (GSS)*, dated July 1, 2007
- ISS-00-001 Revision 0, *Annual Update of System Security Documentation for Automated Information Systems*, dated March 1, 2006
- Project Management Methodology Web site, Roadmap: ISS C&A Deliverables

The agency has not provided any policies or guidance that contradicts the requirement that all major applications and general support systems, even those that are low-impact, require annual contingency plan testing.

15. *Lines 1117-1118. "...the NRC the network..." should be "..the NRC network..."*

The report was modified as suggested.

16. *Lines 1316-1321. Concludes that "…the certifications and accreditations for all the agency's remaining 28 operational systems have expired." For the HRMS and FEES systems, as well as for other systems, new C&A activities have been conducted and are in process.*

    We suggest adding the sentence: "Of these 28 systems, 14 have completed new C&A activities through the security categorization, 9 have completed risk assessments, and 9 are in the security plan phase."

The report was not modified as suggested. The agency has not provided sufficient evidence to support the statement that new C&A activities have been conducted and are in process.

17. *Lines 1402-1419. The report states that the agency may not have an adequate understanding of the threats, risks, and vulnerabilities for systems operating under an interim authority to operate (IATO). For the FEES and HRMS systems operating under an IATO, the risks are*

known as each have approved security categorizations and risk assessments, and security plans have been prepared but are not approved. We suggest noting this in the report.

The report was modified to remove FEES and HRMS from the examples of systems that are currently operating under an IATO.

18. *Page 72, regarding the FEES and HRMS Plan of Action and Milestones (POA&Ms)*

For the FEES System, we request additional information, as we do not have information that supports the statement in the 2nd bullet. FEES POA&M weaknesses related to an IG report were closed this past year, and some were closed because "a decision was made at the agency level not to continue with the C&A on this legacy system undergoing modernization." Please update or remove the bullet.

The agency was provided with the specific POA&M items referred to in the 2nd bullet. The report was modified to clarify the discussion of these particular POA&M items.

For the HRMS weaknesses related to the security plan and the contingency plan, these were closed because an IATO was provided, and it was decided not to invest additional resources in the security plan. The contingency plan has been updated and a test performed. Additionally, we suggest the bullet for HRMS be amended to reflect that "a decision was made at the agency level not to continue with the C&A on this legacy system undergoing modernization."

The report was modified to clarify the discussion of these particular POA&M items.

19. *The FEES system acronym should be used consistently throughout the document.*

All system names in brackets were removed from the discussion draft before the report was submitted as a final.

[Page intentionally left blank]