September 29, 2006

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 2006 (OIG-06-A-26)

Attached please find the Office of the Inspector General's report, *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2006.* This report reflects the results of the independent evaluation performed by Richard S. Carson & Associates, Inc., on behalf of the NRC Office of the Inspector General.

The evaluation determined that the NRC's information security program has significant deficiencies concerning the 1) lack of certification and accreditation, and 2) not performing annual contingency plan testing. This independent evaluation also identified eight information security program weaknesses.

During an exit conference on September 26, 2006, NRC officials provided comments concerning the draft audit report and subsequently opted to submit formal written comments to this report.

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

Attachment: As stated

Electronic Distribution

John T. Larkins, 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
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, 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, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
Michael R. Johnson, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Jack R. Strosnider, 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
Janet R. Schlueter, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV

EVALUATION REPORT

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2006

OIG-06-A-26 September 29, 2006

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

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2006

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

September 29, 2006

[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 the agency's information security program[1] and practices to determine their 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-06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 17, 2006, requires the agency's IG to complete the OMB FISMA Reporting Template for Agency 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, and is included as Appendix C to this report.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on August 31, 2006. 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 2006.

RESULTS IN BRIEF

Program Enhancements and Improvements

To correct weaknesses identified by the FY 2005 FISMA independent evaluation by the NRC Office of the Inspector General (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 will first perform certification and accreditation for 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 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 provides an in-

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

depth discussion of certification and accreditation and its significance to an agency's information security program.

The agency has also accomplished the following since the FY 2005 FISMA independent evaluation:

- The agency developed a comprehensive certification and accreditation process, which is not yet finalized. The agency developed templates for all certification and accreditation documents and instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology.
- The agency completed annual self-assessments for all but 1 of the agency's 30 operational systems, for the four NRC regional offices and the Technical Training Center, and for 4 of 12 contractor systems.
- The agency updated security plans for 3 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 updated risk assessments for 3 of the agency's 30 operational systems. Subsequent to the completion of fieldwork, the agency provided an updated risk assessment for another system.
- The agency developed an approach for consolidation of NRC information systems inventory systems. According to the agency, the reconciliation and consolidation of data from the existing information systems inventory systems is approximately 95 percent complete.

Significant Deficiencies

The following significant deficiencies were identified in NRC's information system security program.

- Only 1 of the 30 operational NRC information systems has a current certification and accreditation, and only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation. The certification and accreditation for the one agency system that was current during this evaluation expires in October 2006.
- Annual contingency plan testing is not being performed.

Program Weaknesses

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

- Different approaches for the security categorization of general support systems result in confusion over responsibility for implementing security controls for high-impact systems.
- The Network Continuity of Operations listed system is incorrectly categorized.
- Known security weaknesses are not being reported on the agency's plans of action and milestones (POA&M).

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 33 of this report.

AGENCY COMMENTS

At an exit conference with the agency held on September 26, 2006, the agency provided informal written comments and generally agreed with the report recommendations. Where appropriate, the OIG modified the report in response to these comments. On September 28, 2006, the agency provided formal written comments, which can be found in Appendix D.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

Carson Associates	Richard S. Carson and Associates, Inc.
CIO	Chief Information Officer
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IATO	Interim Authorization to Operate
IG	Inspector General
IT	Information Technology
LAN/WAN	Local Area Network/Wide Area Network
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

[Page intentionally left blank]

TABLE OF CONTENTS

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 the agency's information security program and practices to determine their 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-06-20 requires the agency's IG to complete the OMB FISMA Reporting Template for Agency 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 2006. This report presents the results of that independent evaluation. Carson Associates also prepared the OMB FISMA Reporting Template for Agency IGs, along with additional narrative, for inclusion in the agency's annual FISMA report. The OMB FISMA Reporting Template for Agency IGs and the additional narrative is included as Appendix C to this report.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on August 31, 2006. 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 2006.

3 Findings

Over the past 4 years, NRC has continued to make 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 FISMA independent evaluation by the 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 will first perform certification and accreditation for 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 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

[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.

process required by FISMA. Section 3.7 provides an in-depth discussion of certification and accreditation and its significance to an agency's information security program.

The first phase of the refocused program included the development of a comprehensive certification and accreditation process, which is not yet finalized. The agency developed templates for all certification and accreditation documents and 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.

The agency has also accomplished the following since the FY 2005 FISMA independent evaluation:

- The agency completed annual self-assessments for all but 1 of the agency's 30 operational systems, for the four NRC regional offices and the Technical Training Center, and for 4 of 12 contractor systems.
- The agency updated security plans for 3 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 updated risk assessments for 3 of the agency's 30 operational systems. Subsequent to the completion of fieldwork, the agency provided an updated risk assessment for another system.
- The agency developed an approach for consolidation of NRC information systems inventory systems. According to the agency, the reconciliation and consolidation of data from the existing information systems inventory systems is approximately 95 percent complete.

The refocused program has not resulted in the completion of a single certification and accreditation despite the (1) emphasis on the certification and accreditation of high priority systems and systems with a higher security risk and (2) application of at least $500,000 in funding to this initiative since December 2005. In the meantime, the certifications and accreditations for all but one of the agency's operational systems have expired.

The following significant deficiencies were identified in NRC's information system security program.

- Only 1 of the 30 operational NRC information systems has a current certification and accreditation, and only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation. The certification and accreditation for the one agency system that was current during the evaluation expires in October 2006.
- Annual contingency plan testing is not being performed.

The independent evaluation also identified eight information system security program weaknesses. Five are repeat findings from the FY 2005 FISMA independent evaluation, and three are new.

- The majority of NRC 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).
- Different approaches for the security categorization of general support systems result in confusion over responsibility for implementing security controls for high-impact systems (new finding).
- The agency does not maintain documentation (certification and accreditation memoranda, self-assessments, and copies of annual contingency plan testing results) that demonstrates systems provided by other Federal agencies meet FISMA requirements (repeat finding).
- Oversight of major applications and general support systems operated by a contractor or other organization on behalf of the agency is lacking (repeat finding).
- The Network Continuity of Operations listed system is incorrectly categorized (new finding).
- E-authentication risk assessments have been completed for only 10 of the agency's 30 operational systems as required by OMB memorandum M-04-04, *E-Authentication Guidance for Federal Agencies* (repeat finding).
- Known security weaknesses are not being reported on the POA&Ms (new finding).
- The agency lacks policies and procedures for ensuring employees with significant information technology (IT) security responsibilities receive security training (repeat finding).

The following sections present the detailed findings from the independent evaluation. As stated previously, some findings are new, and some are repeat findings from the previous FISMA independent evaluation. Only new findings will have a corresponding recommendation. The following sections are organized based on the OMB FISMA Reporting Template for Agency IGs, which can be found in Appendix C. Each major section corresponds to a question or set of questions from the template.

3.1 Total Number of Agency and Contractor Systems

Agency Systems

OMB Requirement	OIG Response
1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (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	3	0
Moderate	8	0
Low	0	0
Not Categorized	19	0
Total	30	0

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, the NRC OIG selected a subset of NRC systems for evaluation during the FY 2006 FISMA independent evaluation. However, during the course of fieldwork, the OIG learned that the re-certification and re-accreditation of these systems, scheduled to be completed by August 2006, would not be completed during the FY 2006 FISMA reporting period. Furthermore, there were no other systems to evaluate because there were only two operational systems with a current certification and accreditation at the time the OIG was selecting systems for evaluation. One of these systems was evaluated by the OIG in FY 2006 and the other system's certification and accreditation expired during the FY 2006 FISMA reporting period. Without enough systems

[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.

with current certifications and accreditations, Carson Associates could not perform an evaluation of a representative subset of agency systems for the FY 2006 FISMA independent evaluation.

A current certification and accreditation is needed to perform a system evaluation because it contains a description of the current planned and in place security controls 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 in place security controls 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, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (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	0	0
Low	1	0
Not Categorized	11	0
Total	12	0

NRC has a total of 12 systems operated by a contractor or other organization on behalf of the agency (8 major applications and 4 general support systems). Of the 12, 7 are operated by other Federal agencies, 2 are operated by federally funded research and development centers, and 3 are operated by private contractors. Carson Associates selected 1 of the 12 systems operated by a contractor or other organization on behalf of the agency for evaluation during the FY 2006 FISMA independent evaluation. However, that system did not have a current certification and accreditation and there was not sufficient information available to perform an evaluation.

FINDING A – Majority of NRC Systems Have Not Been Categorized in Accordance With FIPS 199 (Repeat Finding)

FIPS 199 requires all agencies to categorize their information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. All systems should have been categorized using FIPS 199 by February 2005.

However, despite this requirement, Carson Associates found that the majority of NRC information systems, including systems operated by a contractor or other organization on behalf of the agency, still have not been categorized in accordance with FIPS 199. Specifically, only 11 of the 30 operational NRC information systems have been categorized. Only 1 of the 12 contractor systems has been categorized.[7]

This is a repeat finding from the FY 2005 FISMA independent evaluation. Of the eight security categorizations evaluated in FY 2005 (1) four were updated in FY 2006, (2) three are being revised as part of the re-certification and re-accreditation of their respective systems (two are complete, but have not been approved), and (3) one is for a system that has been combined with another system. In FY 2006, the agency completed another seven security categorizations for NRC systems, and one for a contractor system. According to the agency, the current target date for completing all system security categorizations is the end of calendar year 2006.

Not only is security categorization required by FIPS 199, it is needed to select the minimum security controls for a system as defined in NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*. As a result, the agency cannot determine the appropriate minimum security controls for its information systems and cannot determine whether the current controls for the information systems are adequate. In addition, the agency cannot be assured they are using the correct minimum security control baseline from NIST SP 800-53 when performing its annual self-assessments.

FINDING B – Different Approaches for the Security Categorization of General Support Systems Result in Confusion Over Responsibility for Implementing Security Controls for High-Impact Systems (New Finding)

FIPS 199 states that for an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values from among those security categories that have been determined for each type of information resident on the information system. NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, states that a general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization depending on the criticality or sensitivity of the system and any major applications the general support system is supporting.

[7] The agency has reported that an additional four agency systems have been categorized. However security categorizations for these systems are still under review by the agency or were not approved. Therefore, these systems are not included in the metrics.

The agency has categorized one of its general support systems as a high-impact system. The agency has categorized another general support system as a moderate-impact system. While the majority of the systems supported by the first general support system are categorized as low or moderate, there are a few systems supported by that general support system that are categorized as high. For this reason, this general support system was divided into two subsystems: a general support system for moderate-impact systems and a general support system for high-impact systems. This approach is consistent with NIST guidance.

In order to function in a cost-effective manner suitable for most NRC systems, the other general support system will only process information at a moderate level. Thus, the rational for the moderate-impact security categorization for that system. It is incumbent upon high-impact systems that rely on moderate-impact general support systems to implement the additional controls required by a high-impact categorization. This approach, also consistent with NIST guidance, is often used when an agency has only a few high-impact systems and it would be more cost-effective for the systems with the high-impact security categorization to implement the additional controls. However, this approach is not consistent with the approach taken with the first general support system, resulting in confusion as to who is responsible for implementing the additional controls.

As a result of the different approaches taken when categorizing general support systems, system owners may assume that a general support system is providing controls commensurate with their system's impact level, when in fact the general support system does not. This possible scenario is illustrated in two of the FY 2006 self-assessments for systems that have been categorized as high-impact systems.[8] The security control SI-3, malicious code protection, includes one enhancement at the moderate-impact level, and an additional enhancement at the high-impact level. Both self-assessments reflect the system owners' belief that the second enhancement is implemented at the agency-level, and not by the system. One of the two self-assessments specifically states that this enhancement is "inherited" from the moderate-impact general support system described above, as well as from two other general support systems. However, the self-assessments for those general support systems do not address the second enhancement as the systems were only categorized as moderate-impact systems.

Therefore, it is imperative that the agency clearly identify those additional controls that high-impact systems would not "inherit" from underlying general support systems that have a moderate-impact categorization. It is also imperative that system owners of high-impact systems understand that they are responsible for implementing those additional controls.

[8] Only one of the security categorizations for the two systems whose self-assessments are discussed in the example has been approved by the agency. The self-assessment for the other system was based on a high-impact security categorization.

RECOMMENDATION

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

1. Clearly identify the additional controls that are the responsibility of a high-impact system when a general support system categorized as having moderate-impact supports a high-impact system.

3.2 Agency Performance of FISMA Activities

3.2.1 Certification and Accreditation

OMB Requirement	OIG Response
2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year. *2.a. Number of systems certified and accredited.*	*See Table 3-3 below.*

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

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

Agency Systems

Only 1 of the 30 operational NRC information systems has a current certification and accreditation. The certification and accreditation for this system will expire in October 2006. Section 3.7 of this report discusses the assessment of the agency's certification and accreditation process in detail.

Contractor Systems

Of the 12 systems operated by a contractor or other organization on behalf of the agency, only 4 have been certified and accredited. These four systems are operated by other Federal agencies. Of the remaining eight, three are operated by other Federal agencies, two are operated by federally funded research and development centers, and three are operated by private contractors.

The FY 2005 FISMA independent evaluation found that the agency does not maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements and that oversight for other contractor systems is lacking. Section 3.3 of this report discusses the assessment of the agency's oversight of information systems used or operated by a contractor or other organization on behalf of the agency. Section 3.3 also discusses the current status of recommendations from the FY 2005 FISMA independent evaluation regarding these findings.

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

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, the fact that only 1 of the 30 operational NRC information systems has a current certification and accreditation, and that only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation, constitutes a ***significant deficiency***. This deficiency is not a recent problem. The agency has made little progress in correcting the deficiency, and according to the agency, completion of all outstanding certifications and accreditations is not expected to be completed until 2009.

3.2.2 Security Control Test and Evaluation

OMB Requirement	OIG Response
2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year. *2.b. Number of systems for which security controls have been tested and evaluated in the last 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	3	0	3
Moderate	8	0	8
Low	0	1	1
Not Categorized	18	3	21
Total	29	4	33

Agency Systems

FISMA requires agencies to test and evaluate the security controls of every information system identified in their inventory no less than annually. The necessary depth and breadth of an annual system review depends on several factors such as (1) the potential risk and magnitude of harm to the system or data, (2) the relative comprehensiveness of the most recent past review, and (3) the adequacy and successful implementation of the POA&M for weaknesses in the system. For example, if last year a system underwent a complete certification and accreditation, this year a relatively simple update or maintenance review may be sufficient, provided it has been adequately documented. The FY 2006 FISMA guidance allows agencies to use either (1) NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, or (2) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53 for the specification and assessment of security controls for Federal information systems.

NRC meets the FISMA requirement to test and evaluate the security controls of agency information systems by performing annual self-assessments on the systems. In addition, NRC developed a self-assessment for common controls that are applicable to all NRC systems. NRC performed self-assessments on all agency operational systems with the exception of one general support system. NRC also performed self-assessments on the four NRC regional offices and the NRC Technical Training Center.[9]

Contractor Systems

NRC performed self-assessments on 4 of the 12 systems operated by a contractor or other organization on behalf of the agency. Of the four, two were full self-assessments, and two were site assessments. The remaining 8 systems operated by a contractor or other organization on behalf of the agency are operated by other Federal agencies. As stated previously, the FY 2005 FISMA independent evaluation found that the agency does not maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements. Refer to

[9] The self-assessments for the regional offices and the Technical Training Center were only site assessments. As such, only the physical and environmental, and personal security controls were evaluated as part of the site assessment.

Section 3.3 of this report for a discussion of the current status of recommendations from the FY 2005 FISMA independent evaluation regarding these findings.

3.2.3 Contingency Planning and Testing

OMB Requirement	OIG Response
2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year. *2.c. Number of systems for which contingency plans have been tested in accordance with policy and guidance.*	*See Table 3-5 below.*

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

FIPS 199 Risk Impact Level	Agency	Contractor	Total
High	0	0	0
Moderate	3	0	3
Low	0	1	1
Not Categorized	0	0	0
Total	3	1	4

Agency Systems

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. As of September 1, 2006, Carson Associates had received contingency plan testing results for only 1 of NRC's 30 operational information systems. Subsequent to the completion of fieldwork, the agency provided contingency plan testing results for three additional systems, however the agency has only reviewed and approved the results for two of the additional systems.

Contractor Systems

Of the 12 systems operated by a contractor or other organization on behalf of the agency, only 1 has had its contingency plan tested in the past year.[10] As stated previously, the FY 2005 FISMA independent evaluation found that the agency does not maintain documentation that

[10] Documentation supporting the contingency plan testing for this system was also provided subsequent to the completion of fieldwork.

demonstrates systems provided by other Federal agencies meet FISMA requirements. Refer to Section 3.3 of this report for a discussion of the current status of recommendations from the FY 2005 FISMA independent evaluation regarding these findings.

FINDING D – Annual Contingency Plan Testing Is Not Being Performed (Significant Deficiency)

As stated previously, NIST SP 800-34 states that contingency plans should be tested at least annually. However, despite this requirement, Carson Associates found that only 3 of the agency's 30 operational information systems, and 1 of the agency's contractor systems, have had their contingency plans tested in FY 2006.

This is a repeat finding from the FY 2005 FISMA independent evaluation. The OIG recommended that the agency develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of a system's certification and accreditation. According to the agency, resources have not been available to support completion of annual contingency plan testing (including test reporting and contingency plan update). According to the agency, the current target date for completing contingency plan testing for all agency systems is August 1, 2007. However, the 3rd Quarter FY 2006 POA&Ms submitted to OMB have projected completion dates for contingency plan testing as late as December 2008.

The following is a summary of the status of contingency plan testing for the 30 operational NRC systems:

- 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 3 years.
- Fifteen systems have not had their contingency plans tested in over 2 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.
- Five systems had their contingency plans tested in 2006 (two are still under agency review).

See Appendix B for details on the status of contingency plan testing for all agency operational systems, as well as for one contractor system.

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 in 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 the past two 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 year.

3.3 Oversight of Information Systems Used or Operated by Contractors or Other Organizations

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. Self-reporting of NIST Special Publication 800-26and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.	*Mostly, for example, approximately 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]

[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.

FINDING E – Agency Does Not Maintain Documentation That Demonstrates Systems Provided By Other Federal Agencies Meet FISMA Requirements (Repeat Finding)

The FY 2005 FISMA independent evaluation found that the agency does not maintain documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements. The OIG made three recommendations to address this finding. According to the agency, the scheduled completion date for these recommendations was August 31, 2006.

As of September 1, 2006, the agency had received certification and accreditation memoranda for four of the seven systems provided by Federal agencies. The agency has been working with the offices to assist in acquiring the required documentation for the remaining Federal systems. 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. In a follow-up memorandum to the agency regarding the status of these recommendations, the OIG suggested a possible solution to the problem. The OIG stated that a memorandum from the Federal agencies stating that annual self-assessments and annual contingency plan testing have been completed will be sufficient to meet the intent of the recommendations. The agency is currently working towards obtaining such memoranda.

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

The FY 2005 FISMA independent evaluation also found that oversight of other contractor systems is lacking. The OIG made one recommendation to address this finding. According to the agency, the scheduled completion date for this recommendation is December 29, 2006.

The agency recently learned that development systems are connected to the NRC operational environment via a general support system operated by a contractor, resulting in significant risk to the infrastructure. This recent development illustrates the need to develop policies and procedures for performing oversight of contractor systems as soon as possible.

3.4 Information Systems Inventory

OMB Requirement	OIG Response
3.b.1. The agency has developed an 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.	*Approximately 51-70% complete*
3.b.2. If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	*Missing: Network Continuity of Operations*
*3.c. The OIG **generally** agrees with the Chief Information Officer (CIO) on the number of agency owned systems.*	*Yes*

OMB Requirement	OIG Response
*3.d. The OIG **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*

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.

While FISMA requires agencies to maintain an inventory of only 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.
- **Other** – an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC LAN/WAN.

The FY 2005 FISMA independent evaluation found that the agency's inventory was only 51-70 percent completed because (1) information in the agency's two inventory systems was inaccurate and inconsistent and (2) only one of the two inventory systems contained information on system interfaces. In FY 2005, Carson Associates generally agreed with the CIO on the number of agency owned major applications and general support systems, but did not agree with the CIO on the number of agency owned systems in the listed and other categories. Carson Associates also found that the agency's inventory was not maintained and updated at least annually.

In FY 2006, Carson Associates again generally agreed with the CIO on the number of agency owned major applications and general support systems. However, Carson Associates could not fully evaluate the following questions from the OMB FISMA Reporting Template for Agency IGs, as the agency had not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

- Does the inventory include information on system interfaces? (2nd part of 3.b.1)
- Does the OIG generally agree on the number of agency owned systems? (3.c)
- Is the inventory maintained and updated at least annually? (3.e)

In response to the FY 2005 findings regarding the inventory, the agency developed an approach for consolidation of the agency's inventory systems. According to the agency, the reconciliation and consolidation of the two inventories evaluated in FY 2005 is approximately 95 percent complete. The agency is continuing to work to resolve inaccuracies in the existing inventories, and has estimated that the inventories will be reconciled and ready for upload into the new NRC Systems Inventory and Configuration Database by July 30, 2006. However, as of September 1, 2006, the agency had not demonstrated that the reconciliation has been completed.

FINDING G – The Network Continuity of Operations Listed System Is Incorrectly Categorized (New Finding)

OMB memorandum M-06-20 provides examples of high-impact systems. The memorandum states that all systems identified as "necessary to support agency continuity of operations" are high-impact systems. These systems would include, for example, telecommunications systems identified in agency reviews under OMB's June 30, 2005, memorandum M-05-16, *Regulation on Maintaining Telecommunications Service During Crisis or Emergency in Federally-owned Buildings*.

The agency's Network Continuity of Operations system is currently categorized as a listed system. In accordance with OMB guidance, the Network Continuity of Operations system is a high-impact system, and therefore should be categorized as a general support system, and not a listed system.

RECOMMENDATION

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

2. Re-categorize the Network Continuity of Operations system as a general support system.

3.5 E-Authentication Risk Assessments

OMB Requirement	OIG Response
3.f. 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 human 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.

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

The FY 2005 FISMA independent evaluation found that e-authentication risk assessments had been completed for only 6 of the agency's 27 operational systems.[12] In FY 2005, Carson Associates reviewed the six completed e-authentication risk assessments and found them to be incorrect and inconsistent with the systems' FIPS 199 security categorizations. For example, in some instances, the e-authentication assurance level was incorrectly determined based on the impact levels assigned to the six categories of harm and impact defined in OMB memorandum M-04-04. In other instances, the impact levels assigned to the six categories of harm and impact were not consistent with the FIPS 199 security categorizations of the systems. In FY 2005, the agency stated that e-authentication risk assessments would be "supported under the interim Information Systems Security contract awarded August 11, 2005, and were expected to be completed by December 15, 2005."

However, as of September 1, 2006, the agency had only provided e-authentication risk assessments for 10 of the agency's 30 operational systems, and 1 of the agency's contractor systems. According to the agency, the current target date for completing all outstanding e-authentication risk assessments is July 30, 2007.

3.6 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, for example, approximately 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, for example, approximately 96-100% of the time*
4.c. Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	*Almost Always, for example, approximately 96-100% of the time*
4.d. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	*Almost Always, for example, approximately 96-100% of the time*

[12] In FY 2005, the agency had 27 operational systems. The agency now has 30 operational systems.

OMB Requirement	OIG Response
4.e. OIG findings are incorporated into the POA&M process.	*Almost Always, for example, approximately 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, for example, approximately 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 submitted to 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.

At a more detailed level, NRC uses an internal system to track the progress of more specific corrective actions. These include corrective actions resulting from activities associated with the certification and accreditation process (e.g., risk assessment, security test and evaluation).

The agency has made minimal progress in correcting weaknesses reported on its POA&Ms. The agency has corrected 15 percent of its program level weaknesses, and 22.7 percent of its system level weaknesses. The majority of delays have been caused by delays in completing certifications and accreditations, as described later in this report in Section 3.7.

In assessing the agency's POA&M process, Carson Associates also found that (1) the metrics submitted to OMB often deviated from the actual POA&Ms, (2) the agency is not always following OMB's POA&M guidance, and (3) known security weaknesses are not being reported on the POA&M.

NRC Has Made Minimal Progress in Correcting Weaknesses Reported on Its POA&Ms

The agency carried over a total of 3 program level and 136 system level weaknesses from FY 2005 into FY 2006. The following tables provide statistics from the three FY 2006 POA&Ms the agency has submitted to OMB.

Table 3-6. Program Level POA&Ms Statistics

Quarter	# At Start of Quarter	# New	# Completed	# On-going	# Delayed	# For Start of Next Quarter
Q1	3	10	0	10	3	13
Q2	13	7	5	8	7	15
Q3	* 16	20	2	27	7	34

** A weakness was reported as closed in Q2 in error and was reported correctly as delayed in Q3.

Table 3-7. System Level POA&Ms Statistics

Quarter	# At Start of Quarter	# New	# Completed	# On-going	# Delayed	# For Start of Next Quarter
Q1	136	71	12	100	95	195
Q2	* 194	34	17	107	104	211
Q3	211	14	37	43	145	188

* A weakness that was not IT related was removed from the POA&M.

The following table summarizes the total number of weaknesses included in the FY 2006 POA&Ms, the total number of corrective actions the agency has reported as completed, the total number of corrective actions that are still on-going, and the number of corrective actions whose completion has been delayed.

Table 3-8. Summary of FY 2006 POA&Ms Through the 3rd Quarter

	Total # Weaknesses	Total # Completed	Total # On-going	Total # Delayed	% Completed
Program Level	40	*7 (6)	27	7	15 %
System Level	255	** 66 (58)	43	145	22.7 %

* One program level weakness was reported as closed in error
** Eight system level weaknesses were reported as closed in error

It should be noted that the six program level corrective actions completed in FY 2006 were from previous FISMA reports. However, of the 58 system level corrective actions completed in FY 2006, only 3 were from previous FISMA reports. The following is a summary of the remaining 55 system level corrective actions completed in FY 2006:

- 2 were reported as completed, but are considered not completed by OIG.
- 6 were reported as completed, but the documents related to the weakness have not been reviewed by the agency, or were not approved by the agency.
- 5 were reported as completed due to a re-categorization of the system or because a system was combined with another system.

- 14 of the completed corrective actions were action items to complete monthly status reports required by interim approval to operate memoranda.
- 13 of the completed corrective actions were action items resulting from the agency's annual security reviews (e.g., complete annual self-assessments, complete annual contingency plan testing).
- 15 of the completed corrective actions were action items resulting from other OIG reviews.

Metrics Submitted to OMB Deviate From the Actual POA&Ms

As in FY 2005, Carson Associates found discrepancies between the metrics submitted to OMB and the actual POA&Ms. However, the discrepancies in the metrics are not significant enough to report as a weakness and are due, in part, to the large number of weaknesses being tracked on the agency's POA&Ms.

The Agency Is Not Always Following OMB's POA&M Guidance

As stated previously, the agency is not always following OMB's POA&M guidance. The following are some examples of deviations from OMB's POA&M guidance found on the FY 2006 POA&Ms.

- The agency reported five weaknesses from OIG reports as completed when the OIG still considered the weaknesses as resolved. All but two have been subsequently closed by the OIG.
- The agency reported six weaknesses as completed when the agency had not reviewed and/or approved supporting documentation. In one case, a document was actually not accepted; therefore, the weakness was not actually completed.
- The agency reported nine weaknesses as completed in error. Carson Associates could not determine whether these errors were an oversight, or were because the agency is not verifying that the weaknesses were actually completed.
- Weaknesses with completion dates over a year old are not always removed from the POA&Ms.

While the agency is not always following OMB's POA&M guidance, the agency is using the POA&Ms to track almost all known security weaknesses. Program officials report to the CIO on a quarterly basis on their remediation process. In some cases, program officials are required to report to the CIO on a monthly basis.

FINDING I – Known Security Weaknesses Are Not Being Reported on the POA&Ms (New Finding)

OMB guidance states that agency POA&Ms must reflect known security weaknesses within an agency and shall be used by the agency, program officials, and the IG as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security

performance gaps. However, Carson Associates found that not all known security weaknesses are being reported on the POA&Ms.

Penetration Testing

The agency conducted a penetration test in December 2005. The penetration testing report dated March 29, 2006, included a total of eighteen findings with corresponding recommendations. The most recent POA&Ms do not include all of the recommendations resulting from the December penetration testing. There are some very general corrective actions on the POA&Ms, such as "Review results from Penetration Test, determine necessary actions, and develop task/milestone schedule for task." However, it is not clear which specific recommendations from the penetration testing report are addressed by these corrective actions.

Business Continuity Plan Testing

The findings from two contingency plan tests conducted in 2005, and one contingency plan test conducted in 2006, were not reported on the respective system POA&Ms.

RECOMMENDATION

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

3. Re-evaluate the procedures developed for identifying weaknesses to be tracked to ensure all known security weaknesses are reported on the POA&Ms.

3.7 Certification and Accreditation Process

OMB Requirement	OIG Response
5. Assess the overall quality of the Department's certification and accreditation process.	*Fail*

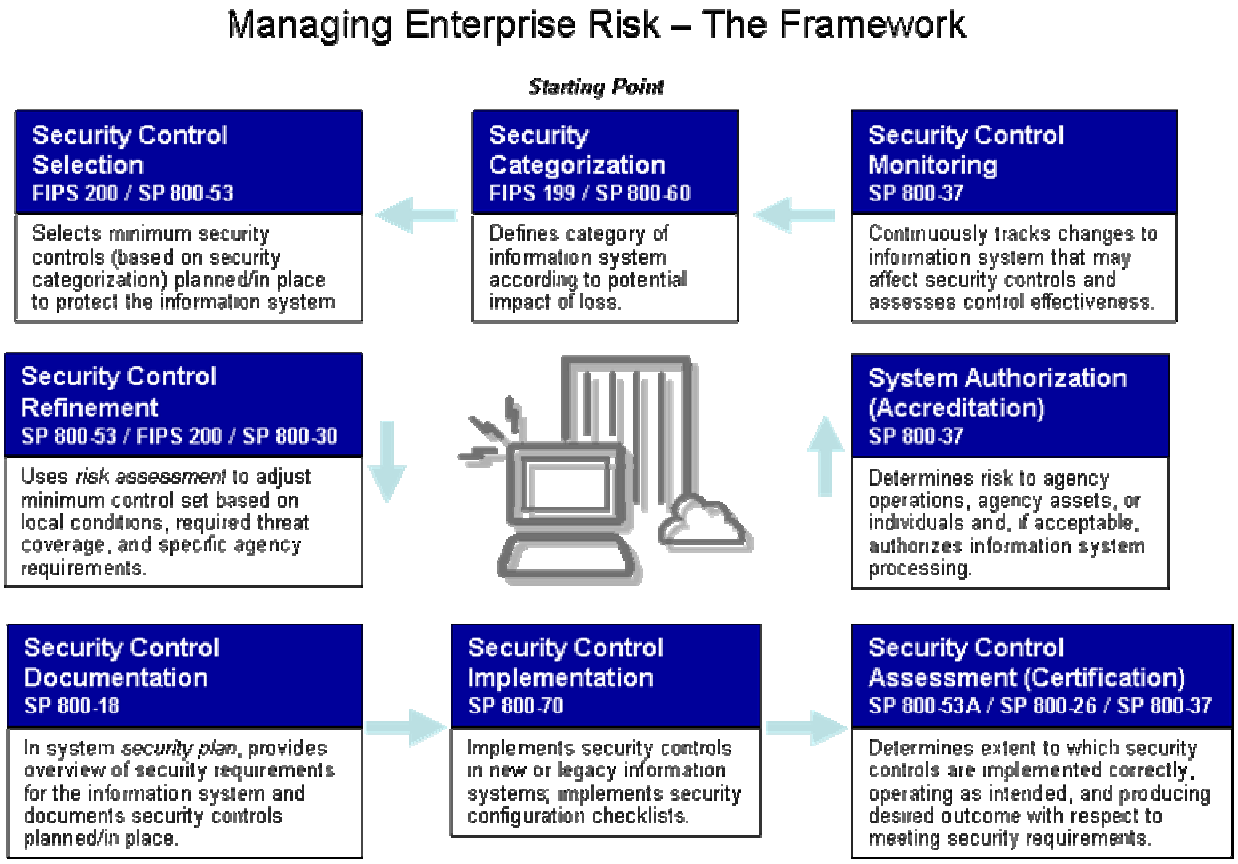
Certification and Accreditation

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,[13] and whenever there is a significant change[14] to the information system or its operational environment.

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

[14] 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.

The following diagram[15] 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. Some of these guidelines and standards were developed only within the past two years, requiring agencies to make changes to their certification and accreditation policies and procedures. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for certification and accreditation.



Security *certification* is a comprehensive assessment of the management, operational, and technical security controls[16] planned and 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

[15] 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).

[16] 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.

information system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official 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) authorization to operate, (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.[17] As a result, potential risks to agency information systems are unknown. Subsequent to the FY 2005 FISMA independent evaluation, the former Chairman directed the agency to submit a plan to refocus the agency's FISMA program for FY 2006 and to submit a plan for an independent review of NRC's FISMA program.

NRC Refocused Information System Security Program

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.

Under the refocused program, the agency will first perform certification and accreditation for 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 include legacy financial systems, two new systems, and infrastructure components supporting these high priority systems. In a December 2005 memorandum to the former Chairman, the agency stated it planned to complete the certification and accreditation for the high priority systems by the following dates:

- Financial systems: second quarter of FY 2006
- One of the new systems: third quarter of FY 2006
- The other new system: first quarter of FY 2007
- Infrastructure components concurrently with the high priority systems

The first phase of the refocused program included the development of a comprehensive certification and accreditation process, which is not yet finalized. The agency developed templates for all certification and accreditation documents and instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology.[18] 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.

The refocused program has not resulted in the completion of a single certification and accreditation despite the (1) emphasis on the certification and accreditation of high priority systems and systems with a higher security risk and (2) application of at least $500,000 in funding to this initiative since December 2005. In the meantime, the certifications and accreditations for all but one of the agency's operational systems have expired. This results in

[17] 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, *Recommended Security Controls for Federal Information Systems*.

[18] The agency's project management methodology is currently in concurrence. The FY 2006 FISMA independent evaluation did not include a review of the new templates, their instructions, or the incorporation of the new certification and accreditation process into the agency's project management methodology. The completion of these activities will be evaluated when they have been finalized and reported as completed to the OIG.

only 1 of the agency's 30 operational systems having a current certification and accreditation, and that certification and accreditation expires in October 2006. As of September 1, 2006, the current target completion dates for certification and accreditation of the high priority systems, and the "pilot," are as follows:[19]

- "Pilot" system: March 2007
- Financial systems: first quarter of FY 2007
- The two new systems: end of FY 2007
- General support system supporting one of the new systems: first quarter FY 2007
- Infrastructure components supporting high priority systems: second quarter FY 2007 and first quarter FY 2008
- Remaining agency operational systems by FY 2009

The FY 2005 FISMA independent evaluation made two recommendations to address the lack of certified and accredited systems; however, the agency is still in the process of implementing those recommendations. According to the agency, the current target date for completing the two recommendations concerning the agency's certification and accreditation process is December 29, 2006.

As stated previously, the fact that only 1 of the 30 operational NRC information systems has a current certification and accreditation, and that only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation, constitutes a ***significant deficiency***.

Independent Review of NRC's Information System Security Program

At the request of the former Chairman, the agency has 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. The evaluation consists of three phases:

- Evaluate the agency's implementation of the certification and accreditation process.
- Perform a needs analysis of the capabilities of the NRC information system security program.
- Benchmark the agency's certification and accreditation process against similarly-sized regulatory and comparable agencies.

The final reports are scheduled for release during the first quarter FY 2007.

[19] The agency stated in their formal written comments that the certifications and accreditations of the six systems that are of highest mission priority will be completed by the end of January 2007.

Issuance of Interim Approvals to Operate Is Not Consistent With NIST Guidance

As stated previously, there are three types of accreditation decisions that can be rendered by authorizing officials: (1) authorization to operate, (2) interim authorization to operate, 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.

NRC 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
- e-Authentication Risk Assessment
- Security Categorization

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. This 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.

- Five systems' last certification and accreditation expired almost a year ago.
- Five systems' last certification and accreditation expired more than 1 year ago.
- One system's last certification and accreditation expired almost 2 years ago.
- Seven 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.
- Three systems have never had a complete certification and accreditation, as they are new general support systems identified when the LAN/WAN was divided into several general support systems. There is insufficient documentation to determine whether these systems are covered by the previous LAN/WAN certification and accreditation.
- Four systems have never had a complete certification and accreditation, but have a security plan and/or risk assessment.
- Four agency systems and two contractor systems have never had a complete certification and accreditation and do not have at least a security plan and 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 or not the risk to agency operations, agency assets, or individuals is acceptable.

As stated previously, the Software Engineering Institute is currently evaluating the agency's certification and accreditation process. The failure to follow NIST guidance when issuing an IATO is one of their preliminary findings.

Agency Funding of New Investments is Inconsistent With OMB Guidance

OMB memoranda M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, and M-06-20 reminded agencies that (1) they must integrate security into and fund security over the lifecycle of each system undergoing development, modernization, or enhancement, and (2) the operations of legacy (steady-state) system operations must meet existing security requirements before new funds are spent on systems development, modernization or enhancement. As an example of this policy in practice, if an agency has a legacy system not currently certified and accredited or for which a contingency plan has not been tested, these actions must be completed before spending funds on a new system.

As stated previously, only one of the agency's legacy systems has a current certification and accreditation, and only three agency systems had their contingency plans tested this year. However, the agency is spending new funds on systems development for several new systems. The following is an example of funds the agency has spent on new systems development.[20]

- Pilot system for electronically storing, processing, and transmitting the agency's safeguards records – $1,374,000

3.8 Security Configuration Policy

OMB Requirement	OIG Response
6.a. Is there an agency wide security configuration policy?	*Yes*
6.b. Are configuration guides available for the products listed in the FY 2006 FISMA Reporting Template?	*Yes*

The agency has implemented several policies that address security configurations and their implementation. In May 2003, the agency developed the NRC System Security Baseline Implementation Plan. Its objective was to establish, develop, implement, maintain, and verify

[20] Dollar figures were obtained from the FY 2007 Exhibit 53 as of January 2006. Dollar figures represent total funds expended through FY 2005.

secure baseline configurations for all information systems. The NRC program is primarily based on the Center for Internet Security's benchmarks and scoring tools. NRC personnel compiled and researched recommended "best practice" technical settings and actions and developed "in house" benchmarks for those platforms for which a benchmark has yet to be developed. The following platforms were the focus of the initiative:

- Microsoft NT
- Microsoft Windows 2000
- Novell NetWare
- Sun Solaris
- IBM AIX
- Linux

The scope of the plan is all NRC systems running the operating systems listed above and includes all systems that are currently in an "active" state and components of the primary NRC network. Subsequent to the implementation of the System Security Baseline Implementation Plan, the agency has begun using the following additional benchmarks and configuration guides.

- Windows 2003 Domain Controllers and Member Servers (Center for Internet Security)
- Microsoft Internet Information Server (National Security Agency)
- Microsoft SQL Server (National Security Agency)
- Router security configuration guide (National Security Agency)
- Cisco router Internet operating system (Center for Internet Security)
- Cisco PIX firewall (Center for Internet Security)
- Apache (Center for Internet Security)
- Oracle (Center for Internet Security)
- Sybase Adaptive Server Enterprise Scoring Tool (NRC developed)

The agency has also posted requirements on the NRC internal IT security Web page for the use of hardening specifications developed by the Center for Internet Security for all systems using the Red Hat Linux operating system. All deviations from the specification must be justified. Areas where the specification says "if absolutely necessary," require justification of the "absolutely necessary" use of the feature. The same applies to the "disable if possible" areas (justify not disabling).

Oracle is currently not in production, but is being tested for planned future production use. Apache is found in the production environment only as a customized version that is bundled with the list manager for the Web interface. Hardening guidelines for the Microsoft Internet Information Server are included with the Windows 2000/2003 configuration guides. HP-UX is found in the production environment, but it is not in widespread use and there is no baseline.

For desktops, NRC has developed a standard image for Windows XP that is based on NIST best practices. NRC uses PatchLink to keep desktop configurations consistent across NRC.

LANDesk can also be used to push upgrades to the desktops. NRC Announcements[21] are used to announce agency workstation updates. The announcements describe the nature of the upgrade and that it will occur via an automated procedure during network login. The announcement includes, as an attachment, the upgrade schedule for each NRC office.

The Office of Information Services also provides the Defense Information Systems Agency Gold Disk tool for the following Windows platforms:

- Windows Server 2003 Member Server
- Windows 2003 Domain Controller
- Windows XP Professional
- Windows 2000 Professional
- Windows 2000 Member Server
- Windows Domain Controller

NRC has also developed system security screening guidelines to prepare new systems for implementation into the NRC production operating environment. The security screening ensures that the system configuration meets 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.

3.9 Incident Detection and Handling Procedures

OMB Requirement	OIG Response
7.a. The agency follows documented policies and procedures for identifying and reporting incidents internally.	*Yes*
7.b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	*Yes*
7.c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT).	*Yes*

Management Directive and Handbook 12.5, *NRC Automated Information Systems Security Program*, 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, externally to law enforcement agencies/officials, and to US-CERT.[22] The most current version of the incident response procedures are maintained on the agency's IT Web site.

[21] NRC Announcements (formerly Network Announcements) communicate information of major significance or interest to agency employees, as well as urgent or time-sensitive information. These announcements do not require signature.

[22] 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.

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.

3.10 Security Awareness and Training

OMB Requirement	OIG Response
8. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?	*Mostly, or approximately 81-95% of employees have sufficient training*
9. 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 General Counsel presents a section on ethics that includes additional discussions on appropriate use of the Internet.

All employees, including contractors, are required to take the online NRC Computer Security Awareness course as soon as they receive a network UserID and every year thereafter. The Office of Information Services maintains a database of personnel who have taken the security awareness course and cross checks the list on a regular basis with an employee list provided by the NRC Office of Human Resources. A Computer Security Team member sends a message to NRC office directors and regional administrators around the first of the month reminding them to have their employees take the course. Information system security officers must sign an acknowledgement of their responsibilities when taking the position and are required to take an online Information System Security Officer training course in addition to the online NRC Computer Security Awareness course. NRC also provides an information systems security course for system administrators.

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 the NRC Computer Security Awareness course annually and by documenting who takes the training, (2) using posters, flyers, Web pages, NRC Yellow Announcements,[23] NRC Announcements, and articles/notices in the NRC monthly newsletter to keep computer security on everyone's mind throughout the year, and (3) holding an Annual NRC Computer Security Awareness Day event.

[23] 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.

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.

Agency staff and contractors are advised of the dangers of peer-to-peer applications during their annual Web-based security training. The online Computer Security Awareness course includes a discussion of the dangers of peer-to-peer applications such as instant messaging. Current agency policy does not explicitly prohibit peer-to-peer applications; however, the agency is blocking sites that support the unauthorized reproduction of copyrighted material, i.e., peer-to-peer and file sharing Web sites.

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

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 costs for providing IT training. The agency's training system does not identify which employees have significant IT security responsibilities and what courses are considered related to IT security. The agency's training system also does 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, receive security training, and the individual and associated training are properly documented and readily identifiable. According to the agency, the current target date for completing the recommendation concerning security training for employees and contractors with significant IT security responsibilities is August 31, 2008.

[Page intentionally left blank]

4 Consolidated List of Recommendations

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

1. Clearly identify the additional controls that are the responsibility of a high-impact system when a general support system categorized as having moderate-impact supports a high-impact system.
2. Re-categorize the Network Continuity of Operations listed system as a general support system.
3. Re-evaluate the procedures developed for identifying weaknesses to be tracked to ensure all known security weaknesses are reported on the POA&Ms.

The following are recommendations from FY 2005 that still remain open that correspond to the repeat findings. These recommendations can be found in OIG-05-A-21, *Independent Evaluation of NRC's Implementation of FISMA for Fiscal Year 2005*.

- Categorize all NRC information systems, including systems operated by a contractor or other organization on behalf of the agency, in accordance with FIPS 199. (Recommendation #1)
- Develop and implement procedures to ensure contingency plans are tested annually, regardless of the status of the systems' certification and accreditation. (Recommendation #3)
- Maintain current copies of certification and accreditation memoranda for systems provided by other Federal agencies. (Recommendation #4)
- Maintain current copies of self-assessments for systems provided by other Federal agencies. (Recommendation #5)
- Maintain current copies of annual contingency plan testing results for systems provided by other Federal agencies. (Recommendation #6)
- 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. (Recommendation #7)
- Review and update the six completed e-authentication risk assessments to correct inaccuracies and inconsistencies with FIPS 199 security categorizations. (Recommendation #8)
- Develop and implement a plan for completing the remaining e-authentication risk assessments. (Recommendation #9)
- 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. (Recommendation #10)

5 OIG Response to Agency Comments

At an exit conference with the agency held on September 26, 2006, the agency provided informal written comments and generally agreed with the report recommendations. Where appropriate, the OIG modified the report in response to these comments. On September 28, 2006, the agency provided formal written comments, which can be found in Appendix D.

SCOPE AND METHODOLOGY

Carson Associates performed an independent evaluation of NRC's Implementation of FISMA for FY 2006. 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 their 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 Systems Security Program*
- NRC Office of the Inspector General audit guidance

This work was conducted between March 2006 and August 2006. Fieldwork ended August 31, 2006. 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; Kelby M. Funn, CISA; and Omar Chaudhry, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]

STATUS OF CONTINGENCY PLAN TESTING

The following information on the status of contingency plan testing was obtained from the 3rd Quarter FY 2006 POA&Ms submitted by the agency to OMB and from working papers from the FY 2005 FISMA independent evaluation. This information is for the 30 operational agency systems as well as for one contractor system.

Table B-1. Status of Contingency Plan Testing

System	Last CP Test Date	Scheduled Test Date	Comment
3-Tier Web	Never tested	Not scheduled	System was put into production without a certification and accreditation. There is no 3rd Quarter FY 2006 POA&M for the system.
ADAMS	August 16, 2004	August 2006	
CTF	June 29, 2004	March 2008	Last test was "inherited" from LAN/WAN.
DCS	April 29, 2004	September 2006	POA&M states testing was completed June 1, 2004.
DDMS	Week of May 15, 2006	Not scheduled	
Desktops	June 29, 2004	June 2008	Last test was "inherited" from LAN/WAN.
E-mail	June 29, 2004	December 2008	Last test was "inherited" from LAN/WAN.
EHD	Never tested	October 2006	
EIE	April 6, 2006	Not scheduled	Agency has not reviewed/ approved test results.
ERDS	May 24, 2004	December 2007	POA&M states testing was completed June 1, 2004.
FEES	August 24, 2006	Not scheduled	
GLTS	May 13, 2004	Task order date + 7.5 months	The system owner will set an actual date upon award of a task order under the new information system security program contract.
HPCS-CDS	Never tested	N/A	Planned transition to listed system by July 30, 2006. As of September 1, 2006, the transition had not occurred.

System	Last CP Test Date	Scheduled Test Date	Comment
HPCS-CFD	Never tested	N/A	Planned transition to listed system by July 30, 2006. As of September 1, 2006, the transition had not occurred.
HRMS	August 21, 2006	Not scheduled	
IDS	June 29, 2004	January 2007	Last test was "inherited" from LAN/WAN.
IPSS	July 25, 2003	June 2007	
LAN/WAN	May 10 and May 11, 2005	September 2006	Test report is dated May 23, 2005.
LSN	April 27-28, 2006	Not scheduled	This is a contractor system.
LTS	May 18, 2004	Waiting for contract award to set date, original date was June 1, 2006	Was to be retired by September 30, 2005. As of September 1, 2006, the system had not been retired.
MPKI	June 29, 2004	September 2006	Last test was "inherited" from LAN/WAN.
Novell Servers	June 29, 2004	November 2007	Last test was "inherited" from LAN/WAN.
NSICD	Never tested	Not scheduled	This is a new system. There is no 3rd Quarter FY 2006 POA&M for the system.
OCIMS	May 24, 2004	July 2006	POA&M states testing was completed September 8, 2004.
RAS	March 27, 2004	Not scheduled	This is another general support system that was broken out from the LAN/WAN. There is no 3rd Quarter FY 2006 POA&M for the system. According to the agency, it was included with the continuity of operations testing performed in March 2004.
RPS	June 28, 2006	Not scheduled	Agency has not reviewed/ approved test results.

System	Last CP Test Date	Scheduled Test Date	Comment
TAC	June 24, 2005	N/A	Planned transition to listed system (once HPCS moves to the production operating environment).
Telecommunications	April 29, 2004	November 30, 2006	Combined DCS/Telecomm POA&M states testing was completed June 1, 2004. This is a general support system that was broken out from the old Data Center/ Telecommunications general support system. There is no 3rd Quarter FY 2006 POA&M for the system.
Unix 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.
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	May 2008	Last test was "inherited" from LAN/WAN.

ADAMS	Agencywide Document Access and Management System
CTF	Consolidated Test Facility
DCS	Data Center Services
DDMS	Digital Data Management System
EHD	Electronic Hearing Docket
EIE	Electronic Information Exchange
ERDS	Emergency Response Data System
FEES	License Fee Reporting System
GLTS	General License Tracking System
HPCS-CDS	High Performance Computing System – Code Development System
HPCS-CFD	High Performance Computing System – Computational Fluid Dynamics System
HRMS	Human Resources Management System

IDS	Intrusion Detection Systems
IPSS	Integrated Personnel Security System
LAN/WAN	Local Area Network/Wide Area Network
LSN	Licensing Support Network
LTS	License Tracking System
MPKI	Managed Public Key Infrastructure
NSICD	NRC Systems Inventory and Configuration Database
OCIMS	Operations Center Information Management System
RAS	Remote Access System
RPS	Reactor Program System
TAC	Technology Assessment Center

FY 2006 OMB FISMA REPORTING TEMPLATE FOR AGENCY IGs

This appendix contains the FY 2006 OMB FISMA Reporting Template for Agency IGs and the additional narrative that will be included with the agency's FISMA submission to OMB.

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: Nuclear Regulatory Commission

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
NRC	High	3	0	0	0	3	0	0	0.0%	3	0.0%	0	0.0%
	Moderate	8	0	0	0	8	0	0	0.0%	8	0.0%	3	0.0%
	Low	0	0	1	0	1	0	0	0.0%	1	0.0%	1	0.0%
	Not Categorized	19	0	11	0	30	0	5	0.0%	21	0.0%	0	0.0%
	Sub-total	**30**	**0**	**12**	**0**	**42**	**0**	**5**	**0.0%**	**33**	**0.0%**	**4**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Agency Totals	**High**	**3**	**0**	**0**	**0**	**3**	**0**	**0**	0.0%	**3**	0.0%	**0**	0.0%
	Moderate	**8**	**0**	**0**	**0**	**8**	**0**	**0**	0.0%	**8**	0.0%	**3**	0.0%
	Low	**0**	**0**	**1**	**0**	**1**	**0**	**0**	0.0%	**1**	0.0%	**1**	0.0%
	Not Categorized	**19**	**0**	**11**	**0**	**30**	**0**	**5**	0.0%	**21**	0.0%	**0**	0.0%
	Total	**30**	**0**	**12**	**0**	**42**	**0**	**5**	0.0%	**33**	0.0%	**4**	0.0%

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and 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. Self-reporting of NIST Special Publication 800-26 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. 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, for example, approximately 81-95% of the time
3.b.1.	The agency has developed an 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: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 51-70% complete
3.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: Network Continuity of Operations Missing Contractor Systems:
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **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.	The agency has completed system e-authentication risk assessments.	No
Question 4		
Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below. For items 4a.-4.f, the response categories are as follows: - 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, for example, approximately 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, for example, approximately 96-100% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 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, for example, approximately 96-100% of the time
Comments: NRC has two primary tools for tracking IT security weaknesses. At a high level, NRC uses the POA&Ms submitted to 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. At a more detailed level, NRC uses an internal system to track the progress of more specific corrective actions. These include corrective actions resulting from activities associated with the certification and accreditation process (e.g., risk assessment, security test and evaluation).		

Question 5	
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. 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 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.	
Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Failing
Comments: See attached narrative, page 4.	

Section C: Inspector General. Questions 1, 2, 3, 4, and 5. Agency Name: Nuclear Regulatory Commission Question 6			
6.a.	Is there an agency wide security configuration policy? Yes or No.		Yes
	Comments:		
6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.		
Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
HP-UX	No	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Linux	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Other. Specify: Novell, AIX, Sybase, SQL Server, Cisco PIX, IIS, Apache	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Comments: W2K Pro is installed only on selected standalone laptops purchased when W2K Pro was the standard Microsoft operating system. These systems are not part of the NRC production operating environment (POE). HP-UX is found in the production environment, but it is not in widespread use and there is no baseline. Oracle configuration guides are available, but this software is currently not in production. Oracle is being tested for planned future production use. Apache configuration guides are also available, but this software is only found in the POE as a customized version that is bundled with the list manager for the Web interface. It is also installed on a development server. IIS hardening guidelines are included in the Windows 2000/2003 configuration guides. There is an IIS 5 configuration guide.			

Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments:		
Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Question 9		
9	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

The following supplemental information is provided in support of the FY 2006 Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) Reporting Template for Agency Inspectors General for the Nuclear Regulatory Commission (NRC). The independent evaluation of NRC's implementation of FISMA for FY 2006 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[24] operational systems that fall under FISMA reporting requirements. [25] Of the 30, 17 are general support systems, and 13 are major applications. As required by FISMA, the NRC OIG selected a subset of NRC systems for evaluation during the FY 2006 FISMA independent evaluation. However, during the course of fieldwork, the OIG learned that the re-certification and re-accreditation of these systems, scheduled to be completed by August 2006, would not be completed during the FY 2006 FISMA reporting period. Furthermore, there were no other systems to evaluate because there were only two operational systems with a current certification and accreditation at the time the OIG was selecting systems for evaluation. One of these systems was evaluated by the OIG in FY 2006 and the other system's certification and accreditation expired during the FY 2006 FISMA reporting period. Without enough systems with current certifications and accreditations, Carson Associates could

[24] 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.

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

not perform an evaluation of a representative subset of agency systems for the FY 2006 FISMA independent evaluation.

Question 1.b. NRC has a total of 12 systems operated by a contractor or other organization on behalf of the agency (8 major applications and 4 general support systems). Of the 12, 7 are operated by other Federal agencies, 2 are operated by federally funded research and development centers, and 3 are operated by private contractors. Carson Associates selected 1 of the 12 systems operated by a contractor or other organization on behalf of the agency for evaluation during the FY 2006 FISMA independent evaluation. However, that system did not have a current certification and accreditation and there was not sufficient information available to perform an evaluation.

Question 2. The metrics in Question 2 represent the status for all NRC systems, not just a subset of systems.

Question 2.a. Only one agency system is certified and accredited, and only four 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, the fact that only 1 of the 30 operational NRC information systems has a current certification and accreditation, and that only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation, constitutes a ***significant deficiency***.

Question 2.b. NRC meets the FISMA requirement to test and evaluate the security controls of agency information system by performing annual self-assessments on the systems. In addition, NRC developed a self-assessment for common controls that are applicable to all NRC systems. NRC performed self-assessments on all agency operational systems with the exception of one general support system. NRC also performed self-assessments on the four NRC regions and the NRC Technical Training Center.

NRC performed self-assessments on 4 of the 12 systems operated by a contractor or other organization on behalf of the agency. The remaining 8 systems are operated by other Federal agencies. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements.

Question 2.c. Only three agency systems had their contingency plans tested in the last year. The agency has reported that two additional major applications had their contingency plans tested in the past year. However, the testing results for these systems are still under review by the agency. Therefore, those systems are not included in the metrics. The agency has also reported that one contractor system had its contingency plan tested in the past year. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements.

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

Question 3.a. NRC presumes that the Federal agencies that operate 8 of the 12 contractor systems are also following FISMA and guidelines from the National Institute of Standards and Technology (NIST). However, the agency is still implementing recommendations from the FY 2005 FISMA independent evaluation to (1) maintain copies of all certification and accreditation documentation for these systems, (2) verify that the security controls have been tested and evaluated for these systems on an annual basis, and (3) verify that the contingency plans have been tested and evaluated for these systems on an annual basis. The agency has been working with the offices to assist in acquiring the required documentation for the contractor 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. In a follow-up memorandum to the agency regarding the status of these recommendations, the OIG suggested a possible solution to the problem. The OIG stated that a memorandum from the Federal agencies stating that annual self-assessments and annual contingency plan testing have been completed will be sufficient to meet the intent of the recommendations. The agency is currently working towards obtaining such memoranda.

The agency is also still developing procedures for performing sufficient oversight and evaluation for contractor systems provided by private contractors to ensure the information systems meet requirements of FISMA, OMB policy, NIST guidelines, and agency policy.

Question 3.b.1. While FISMA requires agencies to maintain an inventory of only major information systems (major applications and general support systems), NRC also tracks two other system types in its inventories – Listed[26] and Other.[27] The FY 2005 FISMA independent evaluation found that the agency's inventory was only 51-70 percent completed because (1) information in the agency's two inventory systems was inaccurate and inconsistent and (2) only one of the two inventory systems contained information on system interfaces. In FY 2006, Carson Associates did not evaluate whether the agency inventory included information on system interfaces as the agency has not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

Question 3.b.2. The agency's Network Continuity of Operations system is currently categorized as a listed system. In accordance with OMB guidance, the NRC Network Continuity of Operations system is a high-impact system, and therefore should be categorized as a general support system, and not a listed system.

[26] A Listed system is 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.

[27] An Other system is an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC local area network/wide area network.

Question 3.c. Carson Associates generally agreed with the CIO on the number of agency owned major applications and general support systems. However, Carson Associates did not fully evaluate the completeness of the agency's inventory, as the agency has not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

Question 3.e. Carson Associates did not fully evaluate whether the agency inventory is maintained and updated at least annually, as the agency has not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

Question 3.f. The FY 2005 FISMA independent evaluation found that e-authentication risk assessments had been completed for only 6 of the agency's 27 operational systems.[28] In FY 2005, Carson Associates reviewed the six completed e-authentication risk assessments and found them to be incorrect and inconsistent with the systems' security categorizations. In FY 2005, the agency stated that e-authentication risk assessments would be "supported under the interim Information Systems Security contract awarded August 11, 2005 and were expected to be completed by December 15, 2005." However, as of September 1, 2006, the agency had only provided e-authentication risk assessments for 10 of the agency's 30 operational systems, and 1 of the agency's contractor systems.

Question 4. While the agency's POA&M process is adequate, the agency has made minimal progress in correcting weaknesses reported on it POA&Ms. The agency has corrected 15 percent of its program level weaknesses, and 22.7 percent of its system level weaknesses. The majority of delays have been caused by delays in completing certifications and accreditations.

Question 5. To correct weaknesses identified by the FY 2005 FISMA independent evaluation 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 will first perform certification and accreditation for those systems that are a high priority from a mission perspective, and those that potentially pose a higher security risk (e.g., agency systems that communicate with systems outside the NRC network). The first phase of the refocused program included the development of a comprehensive certification and accreditation process, which is not yet finalized. The agency developed templates for all certification and accreditation documents and 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.

The refocused program has not resulted in the completion of a single certification and accreditation despite the (1) emphasis on the certification and accreditation of high priority systems and systems with a higher security risk and (2) application of at least $500,000 in funding to this initiative since December 2005. In the meantime, the certifications and

[28] In FY 2005, the agency had 27 operational systems. The agency now has 30 operational systems.

accreditations for all but one of the agency's operational systems have expired. The certification and accreditation for the one agency system that was current during the evaluation expires in October 2006.

As stated previously, the fact that only 1 of the 30 operational NRC information systems has a current certification and accreditation, and that only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation, constitutes a ***significant deficiency***.

Question 8. NRC ensures all employees and contractors receive security awareness and training. However, 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 costs for providing IT training. The agency is still developing procedures for ensuring employees with significant information technology security responsibilities receive security training.

[Page intentionally left blank]

FORMAL AGENCY COMMENTS

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

September 28, 2006

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

FROM: Jacqueline E. Silber
Deputy Executive Director
for Information Services and Administration
and Chief Information Officer
Office of the Executive Director for Operations

SUBJECT: NRC STAFF COMMENTS ON THE OIG'S INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2006

You have provided the Office of the Inspector General's independent evaluation of the U.S. Nuclear Regulatory Commission's implementation of the Federal Information Security Management Act for Fiscal Year 2006. I am providing our written comments on this report for submission with the report.

If you have any questions regarding these comments, please contact Kathy Lyons-Burke, Senior Information Technology Security Officer.

Enclosure:
As stated

cc: Chairman Klein
Commissioner McGaffigan
Commissioner Merrifield
Commissioner Jaczko
Commissioner Lyons
SECY
OGC
OPA
CFO
OIG

CONTACT: Kathy Lyons-Burke, SITSO/OIS
301-415-6595

**NRC STAFF COMMENTS ON THE OIG ANNUAL
FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)
REPORT FOR FY 2006**

The NRC fully supports the requirements for FISMA compliance and believes these activities are essential to protecting the information and resources the agency uses to carry out its mission. NRC systems will be accredited when all appropriate risk-based information technology (IT) security controls are implemented, operating as intended, and produce the desired result. NRC recognized the need to bring better focus to IT security and in July 2005 developed a plan to implement an information system security (ISS) program that ensured a more comprehensive plan for IT system security. That plan was provided to the NRC Commission on July 21, 2005. The plan included early implementation of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, that resulted in an early impact to NRC system certification and accreditation (C&A). However, planning ahead for implementation of these standards poised NRC to be compliant earlier than would otherwise be possible. The plan was accepted by the Commission in December 2005.

The NRC is also taking aggressive and deliberate steps to continue building a sound ISS Program to address the security of NRC's information systems and FISMA compliance shortfalls. Our goal is to provide an effective security program that weighs risk, openness, and cost as an institutionalized part of everyday business practices.

Although the NRC agrees with the majority of the OIG findings, it is important to note that significant work has continued beyond August, 2006. The NRC will: 1) complete security categorizations for all major and general support systems by the end of calendar year 2006 and 2) complete the certification and authorization of six of the systems that are of highest mission priority by the end of January, 2007.

NRC is taking a proactive role in ensuring compliance with new FISMA guidance. NRC is carefully and deliberately building a sound ISS program in a fiscally responsible fashion. In particular, NRC is using NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems and the new NIST SP 800-53, Recommended Security Controls for Federal Information Systems for all NRC major systems to ensure full compliance as soon as possible. However, the NIST SP 800-53 introduced a level of detail and granularity that is significantly greater than what was contained in previous guidance. The review of existing security documentation during the C&A process found that many NRC systems did not contain the level of detail necessary to address the security control requirements of NIST SP 800-53 without significant revision, and system development methodologies did not deliver system and security documentation with the appropriate level of detail required for C&A.

Compliance in a fiscally responsible manner requires establishing standardized security controls for information systems and developing verification procedures for assessing the effectiveness of those controls, as well as effective integration of security C&A with system development processes and more effective delivery of required security documentation and

Enclosure

products. The effort to move toward corporate management of IT and identification of common IT security controls and products to support NRC systems has caused a delay in full system C&A of many NRC systems, particularly legacy systems. However, this proactive approach will ultimately simplify both system development activities and system operations and maintenance while ensuring IT security and full and complete system C&A for all NRC major systems. NRC has focused its efforts on the C&A of those information systems that are a high priority from a mission perspective and/or those that potentially pose a higher security risk, regardless of whether the system is new or is a legacy system. NRC has made significant progress toward FISMA compliance in FY 2006.

NRC has reviewed existing internal practices to identify opportunities to streamline and automate the system C&A process and better integrate the security and system development processes. Modifications to the practices will enable more effective delivery of required security documentation and products, consistent implementation of OMB and NIST guidance, flexible and scalable security processes, and version control and configuration management for all security documentation. NRC is automating our C&A process through the use of an automated tool suite that will facilitate the development of security requirements and documentation, allow for reuse of security information as it flows through the C&A process, and allow close oversight and tracking of security control testing and implementation status. These tools allow integration of agency enterprise architecture, system development, and security processes. NRC has documented the C&A process and the process is available across the agency via an internal web page.

NRC engaged an outside independent contractor to perform an independent review and evaluation of its information assurance C&A process to assess the effectiveness of the NRC ISS Program, better understand effective practices used elsewhere in the Federal government, and identify long-term solutions for the C&A of NRC information systems. NRC has also tasked the independent contractor to conduct a benchmark to compare NRC's ISS Program and C&A process to the practices of two other Federal agencies. The review compares the current state of compliance with FISMA requirements with respect to percent of systems accredited, as well as the quality of documentation and the level of conservatism in the security controls implemented. The review compares the cost of accrediting systems and the process used for C&A with the costs and best practices at the other agencies. The independent review reports will be completed in first quarter FY 2007.

In December 2005, the NRC engaged an outside contractor to conduct an external and internal IT security penetration test against the agency. The purpose of this test was to understand the external presence of the NRC on the Internet, identify security vulnerabilities that could be taken advantage of by hackers over the Internet, identify internal threat sources, assess NRC's compliance with documented policies and procedures, and develop recommendations for fixing and/or addressing vulnerabilities that could be exploited.

The results of the penetration testing identified strong perimeter security practices through deployment of external security measures and controls currently in place. The contractor was unable to obtain a full network mapping of NRC computers, servers, and devices from an external Internet connection due to preventive measures the agency has implemented. The testing identified a number of internal security vulnerabilities, such as network ports not adequately protected, the ability to obtain user network identifications and passwords through social engineering techniques, and the willingness of staff to provide access to workstations

through responses to bogus e-mails. As a follow-on effort, penetration tests were also performed at each NRC regional office and NRC's Technical Training Center during July 2006. Identification of issues from the penetration testing is enabling NRC to address the most significant IT security concerns and take immediate corrective actions. As a result of the social engineering vulnerabilities, NRC has developed in-person IT security training for all NRC users in addition to NRC's annual on-line awareness course. The course is mandatory and will be conducted during the first and second quarters of FY 2007.

NRC has also begun to implement quarterly operating system scans. These scans reveal issues that make systems vulnerable to both external and internal attacks. In order to address some of the most significant issues identified during the scans, NRC has implemented Patchlink. Patchlink enables NRC to push patches out to systems that reside within NRC's infrastructure and enables a much faster implementation of critical IT security patches.

NRC efforts to hire and retain staff resources with the necessary IT security skills has been challenging. In order to complete NRC system C&A the agency has awarded a contract to provide C&A and FISMA support services consistently across the agency. This contract was awarded at the end of July 2006.

NRC has prioritized the C&A of systems based upon the criticality of the systems to NRC's mission. The highest priority systems are being addressed first and most of those systems have completed the security categorization process, the e-authentication risk analyses, and the risk assessment. During the security categorization process, many system owners characterized their systems as having a higher sensitivity than corresponds to federal guidance. NRC brought the sensitivity in line with federal guidance to ensure adequate risk-based IT security controls and thus avoided the significant cost of implementing the IT security controls for a higher sensitivity level. Based upon the risk assessments, NRC is taking corrective action prior to completing the system security plans.

Where NRC relies on another government agency for system services, NRC has made every attempt to review the system C&A documentation and ensure the system is providing adequate IT security controls for the NRC information being processed. In some cases, this has not always been possible.

NRC has made significant strides during FY 2006 to ensure that NRC information and information systems are appropriately secured and to ensure NRC FISMA compliance. The work completed to date, particularly completion of the security categorization, has given us confidence that our understanding of systems is fairly accurate, even though the documentation has not been completed. All efforts have been risk-based and consistent across all NRC systems. NRC believes that with the recently acquired additional contractor resources, NRC will be able to make even more progress over FY 2007.