EVALUATION REPORT

Independent Evaluation of NRC's
Implementation of the Federal
Information Security Management
Act for Fiscal Year 2010

OIG-11-A-03 November 9, 2010

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

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

OFFICE OF THE
INSPECTOR GENERAL

November 9, 2010

MEMORANDUM TO: R. William Borchardt
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 2010 (OIG-11-A-03)

Attached is the Office of the Inspector General's (OIG) report titled, *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2010.*

The report presents the results of the subject evaluation. Agency comments provided during a November 5, 2010, exit conference have been incorporated, as appropriate, into this report.

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

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

Attachment: As stated

Electronic Distribution

Edwin M. Hackett, Executive Director, Advisory Committee
on Reactor Safeguards
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety
and Licensing Board Panel
Stephen G. Burns, General Counsel
Brooke D. Poole, Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Hubert T. Bell, Inspector General
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Michael F. Weber, Deputy Executive Director for Materials, Waste,
Research, State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director
for Corporate Management, OEDO
Martin J. Virgilio, Deputy Executive Director for Reactor
and Preparedness Programs, OEDO
Nader L. Mamish, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Office
Roy P. Zimmerman, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
and Environmental Management Programs
Cheryl L. McCrary, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Catherine Haney, Director, Office of Nuclear Material Safety
and Safeguards
Eric J. Leeds, 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
James T. Wiggins, Director, Office of Nuclear Security
and Incident Response
Marc L. Dapas, Acting Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
Mark A. Satorius, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2010

Contract Number: GS-00F-0001N
Delivery Order Number: 20291

November 05, 2010

[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.[1] FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[2] 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-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010, requires the agency's Office of the Inspector General (OIG) to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

Richard S. Carson & Associates, Inc. (Carson Associates), performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2010. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on September 30, 2010.

PURPOSE

The objective of this review was to perform an independent evaluation of the NRC's implementation of FISMA for FY 2010.

RESULTS IN BRIEF

Program Enhancements and Improvements

Over the past 8 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. The agency has accomplished the following since the FY 2009 FISMA independent evaluation:

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

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

- The agency continued to make significant progress in certifying and accrediting its systems. For the first time since 2001, when reporting on certification and accreditation began under Government Information Security Reform Act (GISRA), all NRC operational systems, including all contractor systems for which NRC has direct oversight, have a current certification and accreditation. In FY 2010, the agency completed certification and accreditation of three existing agency systems and two new systems, and reaccredited four agency systems. As of the completion of fieldwork for FY 2010, all 25 operational NRC information systems and all 3 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation.
- The agency completed or updated security plans for all of the agency's 25 operational systems and for all 3 contractor systems.
- The agency completed annual security control testing for all agency systems and for all contractor systems.
- The agency completed annual contingency plan testing for all but one agency system and for all contractor systems, including updating the contingency plans.
- The agency issued several new Computer Security Office processes including the NRC Agency-wide Continuous Monitoring Program, the NRC Security Impact Assessment Process, and the NRC Plan of Action and Milestones (POA&M) Process.

Program Weakness

While the agency has continued to make improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified one information system security program weakness – a repeat finding from several previous independent evaluations: the agency's POA&M program still needs improvement.

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 39 of this report.

AGENCY COMMENTS

At an exit conference on November 5, 2010, agency officials agreed with the report's findings and recommendations and provided a few editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

ABBREVIATIONS AND ACRONYMS

Carson Associates	Richard S. Carson & Associates, Inc.
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
DISA	Defense Information Systems Agency
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GISRA	Government Information Security Reform Act
IAS	Information Assurance System
IATO	Interim Authorization to Operate
IG	Inspector General
ISS	Information System Security
ISSO	Information Systems Security Officer
IT	Information Technology
LoB	Line of Business
MD	Management Directive
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSICD	NRC System Information Control Database
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PMM	Project Management Methodology
POA&M	Plan of Action and Milestones
SCAP	Security Content Automation Protocol
SGI	Safeguards Information
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 Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program 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-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated April 21, 2010, requires the agency's Office of the Inspector General (OIG) to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

Richard S. Carson & Associates, Inc. (Carson Associates), performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2010. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on September 30, 2010.

2 Purpose

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2010. The appendix contains a description of the evaluation scope and methodology.

3 Findings

Over the past 8 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. The agency has accomplished the following since the FY 2009 FISMA independent evaluation:

- The agency continued to make significant progress in certifying and accrediting its systems. For the first time since 2001, when reporting on certification and accreditation began under the Government Information Security Reform Act (GISRA), all NRC operational systems, including all contractor systems for which NRC has direct oversight, have a current certification and accreditation. In FY 2010, the agency completed certification and accreditation of three existing agency systems and two new systems, and reaccredited four agency systems. As of the completion of fieldwork for FY 2010, all 25 operational NRC information systems and all 3 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation.

- The agency completed or updated security plans for all of the agency's 25 operational systems and for all 3 contractor systems.
- The agency completed annual security control testing for all agency systems and for all contractor systems.
- The agency completed annual contingency plan testing for all but one agency system and for all contractor systems, including updating the contingency plans.
- The agency issued several new Computer Security Office (CSO) processes including the NRC Agency-wide Continuous Monitoring Program, the NRC Security Impact Assessment Process, and the NRC Plan of Action and Milestones (POA&M) Process.

While the agency has continued to make improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified one information system security program weakness – a repeat finding from several previous independent evaluations: the agency's POA&M program still needs improvement.

The following sections present the detailed findings from the independent evaluation and are organized based on the OIG section of the OMB FISMA reporting tool. Beginning with Section 3.2, each major section corresponds to a question or set of questions from the IG section of the OMB FISMA reporting tool. Each section is introduced with a table that contains the OMB requirement as stated in the OMB FISMA reporting tool . Findings are presented in the sections to which they are relevant.

3.1 FISMA Systems Inventory

For FY 2010, OMB did not ask the OIGs to provide an evaluation of the quality of the agency's system inventory. However, as FISMA requires agencies to develop and maintain an inventory of major information systems operated by or under the control of such agency, this evaluation includes an assessment of the NRC system inventory to determine if it meets FISMA requirements.

As of completion of fieldwork, NRC had 25 operational systems that fall under FISMA reporting requirements.[3] Of the 25, 8 are general support systems,[4] and 17 are major applications.[5] NRC had three systems operated by a contractor or other organization on behalf of the agency (one major application and two general support systems). Of the three, one is operated by a federally funded research and development center, and two are operated by private contractors. As required by FISMA, Carson Associates selected a subset of NRC systems and contractor systems for evaluation during the FY 2010 FISMA independent evaluation.

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

[4] 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.

[5] 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.

Table 3-1. Total Number of Agency and Contractor Systems and Number Reviewed by FIPS 199 System Impact Level

	Agency Systems		Contractor Systems		Total Number of Systems (Agency and Contractor Systems)	
FIPS 199 System Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
High	9	1	1	1	10	2
Moderate	16	2	1	0	17	2
Low	0	0	1	0	1	0
Not Categorized	0	0	0	0	0	0
Total	25	3	3	1	28	4

Agency System Inventory – Background

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.

Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, also define requirements for the agency's inventory of automated information systems. The agency's inventory must identify all interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. MD and Handbook 12.5 also require the agency Chief Information Officer (CIO) to establish procedures for interconnection of any information technology (IT) device or system with the NRC IT infrastructure systems. MD and Handbook 12.5 also specify requirements for connections to the NRC network infrastructure. Written management authorization is required before establishing a connection between the NRC IT infrastructure and another system that is not NRC controlled. Connections to other Government-owned systems also may require the establishment of a memorandum of understanding (MOU).

To address findings from previous independent evaluations regarding the agency's inventory, the agency developed an automated inventory system, the NRC System Information Control Database (NSICD), to house the inventory of automated information systems. The agency inventory is maintained and updated at least annually. The agency issues data calls twice a year, typically in January and August. Data call packages include an explanation of the data fields found on the data call inventory sheets and instructions on how to verify and enter the data. The agency also developed several procedures and guides to assist NRC offices with the data calls and to assist the agency in maintaining the inventory data in NSICD.

The NRC Inventory Interface Information Meets FISMA Requirements

The FY 2008 FISMA independent evaluation found that very little interface information was included in NSICD and that the interface information in NSICD was inconsistent with the interface information included in system security plans. In response to recommendations from the FY 2008 independent evaluation, the agency updated NSICD to include interface information for all systems in the NRC inventory. The agency also developed a guide for the CSO administrative staff for entering data into security records within NSICD to ensure interface information is consistent with interface information in security plans and risk assessments. However, the FY 2009 FISMA independent evaluation found that the majority of the interface was still inconsistent with information found in IT security documentation, as well as with interface information within NSICD. While there was more interface information in NSICD than was found during the FY 2008 independent evaluation, the information was still incomplete and inconsistent.

The FY 2009 FISMA independent evaluation recommended that the two recommendations from the FY 2008 FISMA independent evaluation regarding system interfaces remain open until the agency corrected the inconsistencies that still existed in the inventory information in NSICD and until the procedures developed to ensure interface information in NSICD is consistent with interface information in security plans and risk assessments are further refined. The FY 2009 FISMA independent evaluation further recommended that the agency develop and implement procedures to ensure interface information is kept up-to-date. The agency completed updating interface information in NSICD with the most recent security plans and updated the *NRC Administrative Guide for Entering Data into NSICD* with additional guidance on entering interface information into NSICD, including procedures to ensure interface information is kept up-to-date. The agency's continuous monitoring program also includes requirements for reviewing system interfaces.

Carson Associates reviewed security plans for 11 systems to identify the interfaces for those systems. Carson Associates then reviewed the records for those systems in NSICD to determine if the agency's inventory included the interfaces identified in the security plans. Carson Associates also analyzed the interface information in NSICD for consistency within the inventory. For example, if system 1 listed interfaces with systems 2, 3, and 4, then those systems should also list an interface with system 1.

Carson Associates found that the majority of the interface information for the 11 systems reviewed was consistent with information found in IT security documentation, as well as with interface information within NSICD, and that the interface information was up-to-date.

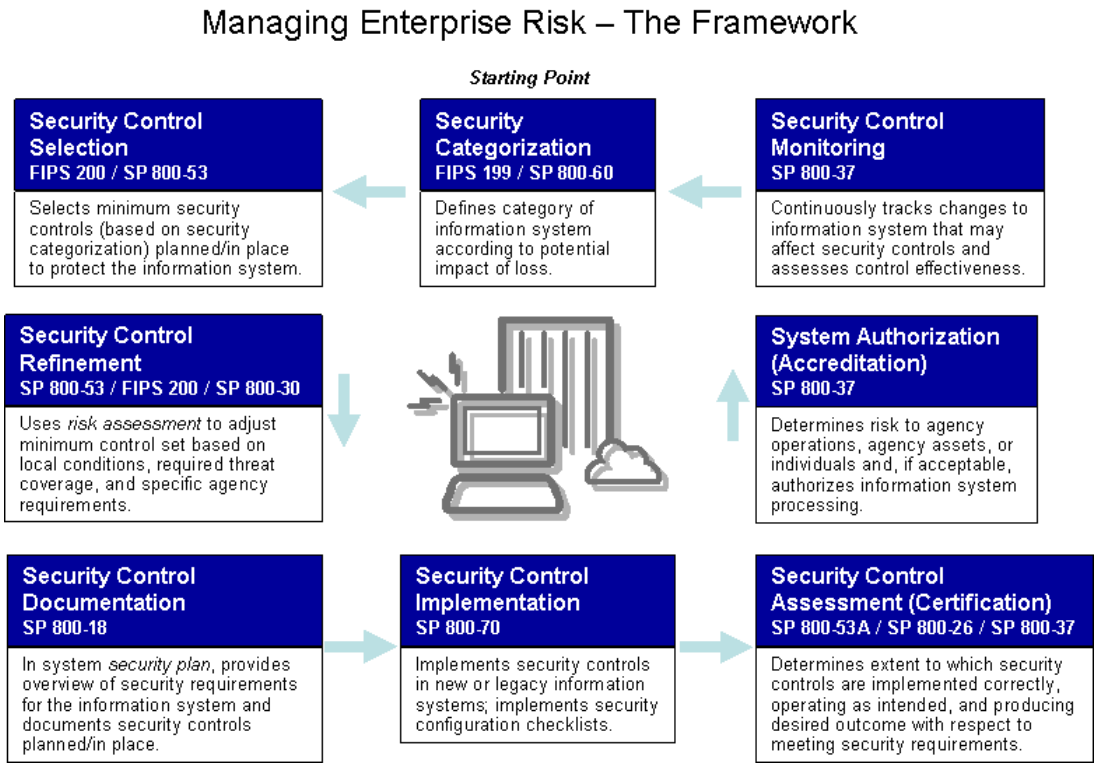
3.2 Status of Certification and Accreditation Program (Question 1)

OMB Requirement	OIG Response
1a. The Agency has established and is maintaining a certification and accreditation program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following eight attributes: *1. Documented policies and procedures describing the roles and responsibilities of participants in the certification and accreditation process.* *2. Establishment of accreditation boundaries for agency information systems.* *3. Categorizes information systems.* *4. Applies applicable minimum baseline security controls.* *5. Assesses risks and tailors security control baseline for each system.* *6. Assessment of the management, operational, and technical security controls in the information system.* *7. Risks to Agency operations, assets, or individuals analyzed and documented in the system security plan, risk assessment, or an equivalent document.* *8. The accreditation official is provided (i) the security assessment report from the certification agent providing the results of the independent assessment of the security controls and recommendations for corrective actions; (ii) the plan of action and milestones from the information system owner indicating actions taken or planned to correct deficiencies in the controls and to reduce or eliminate vulnerabilities in the information system; and (iii) the updated system security plan with the latest copy of the risk assessment.*	X
1b. The Agency has established and is maintaining a certification and accreditation program. However, the Agency needs to make significant improvements as noted below.	
1c. The Agency has not established a certification and accreditation program.	

Certification and Accreditation – Background

The security certification and accreditation of information systems is integral to an agency's information security program and is an important activity that supports the risk management process required by FISMA. Information systems under development must be certified and accredited prior to becoming operational. Operational information systems must be recertified and reaccredited every 3 years in accordance with Federal policy[6] and whenever there is a significant change[7] to the information system or its operational environment.

The following diagram[8] 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, the National Institute of Standards and Technology (NIST) has developed several standards and guidelines to support the management of enterprise risk. NIST Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for certification and accreditation.



[6] OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*.

[7] Examples of significant changes to an information system that should be reviewed for possible reaccreditation 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 reaccreditation action.

[8] 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).

Security *certification* is a comprehensive assessment of the management, operational, and technical security controls[9] that are planned or in place in an information system to determine the extent to which the controls are (1) implemented correctly, (2) operating as intended, and (3) producing the desired outcome with respect to meeting the security requirements for the information system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official[10] 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.

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

[10] The agency refers to the authorizing official as the designated approving authority. OMB refers to the authorizing official as the accreditation official.

- **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 NRC Certification and Accreditation Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's certification and accreditation program, Carson Associates reviewed the certification and accreditation process and procedures located on the agency's project management methodology (PMM) Web site, and reviewed accreditation decision memoranda issued by the agency's authorizing official. NRC's certification and accreditation program is documented on its PMM Web site and is part of the agency's Information System Security (ISS) program. The objectives of the ISS program are to:

- Implement appropriate security measures to protect NRC information and information systems.
- Ensure that security measures provide the appropriate level of protection and reliable access to NRC information and information systems by authorized individuals, and only by authorized individuals, and operate as intended.
- Ensure that senior agency officials exercise due diligence over information security for the information and information systems that support the operations and assets under their control.

The PMM Web site includes workflows for the authority to operate process and the continuous monitoring process. Each workflow includes a work breakdown structure, team allocations, and work product usage information. The PMM Web site includes templates for all required certification and accreditation artifacts. The PMM Web site also includes guidance on the use of common and inheritable controls.

To determine if the agency is managing and operating a certification and accreditation program in compliance with its policies, we reviewed the certification and accreditation documents for the four systems selected for evaluation during the FY 2010 independent evaluation. We also reviewed the agency's continuous monitoring process, including the requirement for annual security control testing, annual contingency plan testing, and annual security plan updates. Carson Associates found that the certification and accreditation documents for the four systems selected for evaluation were in compliance with agency policy, with a few minor deviations. The agency has been provided detailed information on any deviations from policy that were identified. Based on certification and accreditation documents that were reviewed, Carson Associates determined that the NRC certification and accreditation program includes the eight attributes specified in the OMB requirement.

Carson Associates also determined that for the four systems selected for evaluation, the authorizing official was presented with the security assessment report, the POA&M, and the updated security plan with the latest copy of the risk assessment.

All NRC Systems Have a Current Certification and Accreditation

Previous evaluations found that the majority of NRC information systems were not certified and accredited. The lack of certification and accreditations for the majority of the agency's systems was reported as a significant deficiency in the FY 2006 and FY 2007 FISMA independent evaluation reports. In FY 2008, just over half of the agency's operational NRC information systems, including all contractor system for which NRC has direct oversight, had a current certification and accreditation. In FY 2009, all but one of the operational NRC information systems had a current certification and accreditation, and all three contractor system for which NRC has direct oversight had a current certification and accreditation.

In FY 2010, the agency completed certification and accreditation of three agency systems and two new systems, and recertified and accredited four agency systems.

For the first time since 2001, when reporting on certification and accreditation began under GISRA, all NRC operational systems, including all contractor system for which NRC has direct oversight, have a current certification and accreditation.

Table 3-2. Total Number of Systems and Number Reviewed That Have a Current Certification and Accreditation by FIPS 199 System Impact Level

FIPS 199 System Impact Level	Agency	Contractor	Total Number	Number Reviewed
High	9	1	10	2
Moderate	16	1	17	2
Low	0	1	1	0
Not Categorized	0	0	0	0
Total	25	3	28	4

3.3 Status of Security Configuration Management (Questions 2 and 3)

OMB Requirement	OIG Response
2a. The Agency has established and is maintaining a security configuration management program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following six attributes *1. Documented policies and procedures for configuration management.* *2. Standard baseline configurations.* *3. Scanning for compliance and vulnerabilities with baseline configurations.* *4. FDCC baseline settings fully implemented and/or any deviations from FDCC baseline settings fully documented.* *5. Documented proposed or actual changes to the configuration settings.* *6. Process for the timely and secure installation of software patches.*	X
2b. The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.	
2c. The Agency has not established a security configuration management program.	

FISMA requires agencies to develop policies and procedures that ensure compliance with minimally acceptable system configuration requirements as determined by the agency. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, requires organizations to (1) establish mandatory configuration settings for information technology products employed within the information system, (2) configure the security settings of information technology products to the most restrictive mode consistent with operational requirements, (3) document the configuration settings, and (4) enforce the configuration settings in all components of the information system.

The agency has also posted guidance on the NRC internal Web site requiring the use of hardening specifications for the different operating systems and software in use at the agency. Hardening specifications in use at the agency include benchmarks developed by the Center for Internet Security (CIS), the Defense Information Systems Agency (DISA) Gold Disk,[11] National Security Agency (NSA) security configuration guides, and custom hardening specifications developed by the agency. The NRC requires the use of standard baseline configurations for any information system that stores, transmits/receives, or processes NRC information. In the absence of CSO-defined standard baseline configurations, the agency allows DISA standards, checklists, and guidance to be used. In the absence of both CSO and DISA configuration information, the agency allows CIS benchmarks to be used.

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

The NRC Security Configuration Management Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's security configuration management program, Carson Associates reviewed the configuration management process and procedures located on the agency's PMM Web site, and reviewed draft configuration management guidelines and processes currently in development. To determine if the agency's configuration management program includes the six attributes specified in the OMB requirement, in addition to the agency's configuration management guidelines and processes, we reviewed the certification and accreditation documents for the four systems selected for evaluation during the FY 2010 independent evaluation.

Documented Policies and Procedures

NRC maintains an agency Master Configuration Management Plan that defines the configuration management procedures for NRC projects from inception to decommissioning. The Master Configuration Management Plan outlines the use of Rational ClearCase for version control and change management for all software projects at NRC. The approach and processes for managing and versioning configuration items associated with systems and application during the operations and maintenance phase of its lifecycle are described. The Master Configuration Management Plan is disseminated via the agency Intranet. The NRC certification and accreditation program requires all systems to have a security plan that includes supporting documents such as a configuration management plan.

The agency is in the process of updating its configuration policies and procedures and has issued the following draft guidance and processes:

- CSO-GUID-1315, NRC Configuration Management Guidance.
- CSO-PROS-1316, Configuration Change Control.
- CSO-PROS-1317, Configuration Item Identification and Documentation.
- CSO-PROS-1319, Configuration Audit and Review.

Standard Baseline Configurations

The NRC requires the use of standard baseline configurations for any system that stores, transmits/received, or processes NRC information. The CSO has developed the following standard baseline configurations:

- NRC Blackberry Enterprise Server and Handheld Configuration Standard.
- Stealth MXP Thumb Drive Configuration Standard.
- NRC Classified Laptop Configuration Standard.
- NRC Safeguards Information (SGI) Laptop Configuration Standard.
- NRC General Laptop Configuration Standard.
- NRC General Laptop Configuration Guidance.

- Linux Red Hat Hardening Guidelines.
- VMWare ESX Server Hardening Guidelines.
- Microsoft Windows 2003 Servers.
- Microsoft Windows 2008 Servers.
- Microsoft SQL Server 2005/2008 Configuration Standards.
- Network Multi-Function Device and Printer Configuration Standards.
- NRC Web 2.0 Implementation Standard.
- NRC YouTube Standard.

In the absence of CSO-defined standard baseline configurations, the agency allows DISA standards, checklists, and guidance to be used. In the absence of both CSO and DISA configuration information, the agency allows CIS benchmarks to be used.

Scanning for Compliance and Vulnerabilities

To determine if the agency is scanning for compliance and vulnerabilities with baseline configurations, Carson Associates reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2010. Carson Associates also examined the vulnerability assessment reports prepared in support of security test and evaluation for the four systems.

The agency performs a vulnerability assessment during security control testing, which includes vulnerability scans, penetration tests, and hardening checks using the following tools:

- Cenzic Hailstorm – A Web application security testing tool to assess the implementation of Web application security policies.
- CIS Benchmarks – NRC-approved security hardening specifications for a variety of platforms and software, prepared by CIS (http://www.cisecurity.org/).
- CORE Impact Penetration Testing Tool – A specialized penetration testing tool that provides automated testing of known exploits against detected platforms, protocols, and services.
- DISA Gold Disk – A Department of Defense tool that tests Windows-based hosts for compliance with the DISA Gold standard, including file and registry access control and auditing settings, running services, installed applications and patches, and user rights.
- nCircle – A vulnerability scanning tool to assess configurations, applications, vulnerabilities, and system integrity. nCircle supports automated compliance checklists and remediation using the Federal Government's Security Content Automation Protocol (SCAP).
- NRC Hardening Guidelines – Agency approved best practices customized for the implementation of secure configurations on information systems unique to the NRC.
- NSA Guides – Guides containing recommended security settings for certain platforms, prepared by NSA.

- Tenable Nessus Vulnerability Scanner – A general-purpose scanning tool that provides information on network-based vulnerabilities.
- ThreatGuard – A vulnerability scanning tool to assess Federal Desktop Core Configuration (FDCC) compliance. ThreatGuard supports automated compliance checklists and remediation using the Federal Government's SCAP.

FDCC Baseline Settings and Deviations

Carson Associates reviewed several agencywide announcements and determined that the agency has adopted and implemented FDCC standard configurations. Carson Associates reviewed the agency's FDCC compliance reports to OMB and to NIST and determined that the agency has documented deviations. For example, on April 6, 2009, the agency's designated approving authority approved a deviation from FDCC regarding password aging. The agency adjusted the FDCC password to a longer time period (from 60 to 90 days) while retaining the existing minimum password length and password complexity requirements. The rationale for the change was to reduce the burden on the user community associated with the shorter password age.

In response to a recommendation regarding the implementation of FDCC at NRC from the FY 2008 FISMA independent evaluation, the CSO in coordination with the Office of Information Services (OIS) developed the following standards and provided them on the CSO Web page:

- Configuration standards for NRC laptops.
- Guidance for general laptops.
- Procedures for applying critical updates to SGI laptops.
- An SGI Stand Alone Listed System Minimum Security Checklist to ensure appropriate laptop configuration.
- Standard system security plans for NRC laptops.
- Laptop security policy provided via memorandum to office directors and regional administrators and yellow announcement to staff.

OIS procedures require the use of standard images for desktop and laptop computers. All computers connected to the NRC network receive FDCC settings through the use of group policy object settings.[12] Computers that are not attached to the network (standalone systems) are loaded with these controls as part of the standard configuration image and additional controls are implemented through local security policy.

In addition, the agency uses NIST-validated SCAP scanning tools to verify that the agency is compliant with FDCC for both OIS centrally managed and region/program office managed computer assets. CSO runs the NIST approved scanning tools against the agency's image for standalone computers and against the agency's general support systems and major applications

[12] Group policy is a feature of Microsoft's operating systems and is a set of rules that control the working environment of user and computer accounts. It provides centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment. Active Directory is a feature of Microsoft's operating systems that provides a variety of network services.

during system certification and accreditation and throughout continuous monitoring and quarterly security scanning, as required by FISMA. The CSO is currently fielding its Information Assurance System (IAS) to provide real-time assessment of FDCC compliance for networked computers as part of its continuing monitoring assurance activities. The completion of the IAS will provide agencywide, real-time FDCC assessments. The SCAP and FDCC compliance tools will be part of the CSO IAS, which is scheduled to be deployed early FY 2011.

CSO updated the continuous monitoring process to include criteria to evaluate system owner compliance with required security controls. The annual continuous monitoring reviews of each office and their respective systems includes an assessment of the implementation of required security controls on standalone PCs and laptops. FDCC configurations are now required for all Microsoft Windows XP Professional installations that connect to the NRC network either internally or remotely. All standalone workstations/laptops must meet the NRC laptop configuration standards.

Documents Proposed or Actual Changes to Configuration Settings

To determine if the agency documents proposed or actual changes to configuration settings, Carson Associates reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2010, specifically the test results for the CM-3 control, Configuration Change Control. This control requires organizations to authorize, document, and control changes to the information system. Of the four systems reviewed, this control was in place for three systems and planned for one system. The control was not in place for the one system primarily because the process for approving changes to configuration settings was not documented. The actual changes themselves are documented. Based on our review of the security test and evaluation results, the agency documents proposed or actual changes to configuration settings.

Process for Timely and Secure Software Patch Installation

To determine if the agency has a process for timely and secure software patch installation, Carson Associates reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2010, specifically the test results for the SI-2 control, Flaw Remediation. This control requires organizations to identify, report, and correct information system flaws. Of the four systems reviewed, this control was in place for one system, planned for two systems, and not applicable for one system. The agency is in the process of remediating the missing patches identified during testing for one system, with a target completion date of March 2011, and has recently completed the system-specific procedures for detecting, recording, and correcting information system flaws for the other system in which this control was identified as inadequate.

In addition, the agency uses the System Center Configuration Manager patch management system to keep desktop configurations consistent across NRC. Network Bulletins are used to announce agency workstation updates. The announcements describe the nature of the upgrade and whether or not a workstation restart is required after the patches are installed. Many other agency systems rely on the agency's IT infrastructure system for patch installation.

Based on our review of the security test and evaluation results, the agency has a process for timely and secure software patch installation.

Baselines Reviewed (Question 3)

To identify which baselines to review, Carson Associates identified the following operating systems, platforms, and systems in use in the four systems selected for evaluation in FY 2010 by reviewing the system security plans, security test and evaluation plans and reports, security assessment reports, vulnerability assessment reports, risk assessments, and other system security documentation:

- Cisco IOS.
- HP-UX.
- Microsoft Internet Information Services.
- Microsoft SQL Server 2000.
- Microsoft SQL Server 2005.
- Microsoft Windows Server 2000.
- Microsoft Windows Server 2003.
- Novell NetWare.
- Novell eDirectory.
- Red Hat Linux.
- Windows XP.

Carson Associates then reviewed the baselines in use by NRC relevant to the above listed operating systems, platforms, and systems. While the agency has established required baselines for additional operating systems, platforms, and systems, Carson Associates could only form an opinion on the baselines for those operating systems, platforms, and systems found in the four systems selected for evaluation in FY 2010.

3.4 Status of Incident Response and Reporting Program (Question 4)

OMB Requirement	OIG Response
4a. The Agency has established and is maintaining an incident response and reporting program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following five attributes: *1. Documented policies and procedures for responding and reporting to incidents.* *2. Comprehensive analysis, validation and documentation of incidents.* *3. When applicable, reports to US-CERT within established timeframes.* *4. When applicable, reports to law enforcement within established timeframes.* *5. Responds to and resolves incidents in a timely manner to minimize further damage.*	X
4b. The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below.	
4c. The Agency has not established an incident response and reporting program.	

FISMA requires agencies to develop, document, and implement an agencywide information security program that includes procedures for detecting, reporting, and responding to security incidents.

On May 2, 2008, the agency issued a revised policy on computer security incident response and personally identifiable information (PII) incident response. The policy provides direction for responding to computer security incidents affecting the NRC's systems, networks, and users, as well as PII incidents and will be included in the next revision of MD and Handbook 12.5. The revised policy contains timeframes for responding to incidents, based on the criticality of the affected resources and the incident; formally establishes a Computer Security Incident Response Team (CSIRT) to respond to incidents; and outlines the CSIRT's security incident response process. The CSIRT includes staff from the following offices: CSO, OIS, Office of Administration, and Office of Nuclear Security and Incident Response. The policy also specifies when the OIG should be involved in addressing a computer security incident.

The NRC Incident Response and Reporting Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's incident response and reporting program, Carson Associates reviewed the agency's policies, procedures and guidance related to incident response and reporting. To determine if the agency's incident response and reporting program includes the five attributes specified in the OMB requirement, in addition to the agency's incident response and reporting policies, procedures, and guidelines, we reviewed the annual security control test

report for the agency's common controls. Incident response policies and procedures are provided at the agency level for all NRC information systems.

In addition to issuing the revised policy on computer security incident response and PII incident response and forming CSIRT, the agency developed the following policies and guidelines related to detecting, reporting, and responding to security incidents. These documents include guidance on reporting incidents internally, reporting incidents to US-CERT, and reporting to law enforcement.[13]

- Information Systems Security Incident Response Procedures, May 11, 2004 (Appendix B from MD and Handbook 12.5).
- CSIRT Responder Guide, Version 1.2, August 4, 2009.
- CSIRT Standard Operating Procedures, Version 1.0, October 30, 2008.

The CSO also maintains an incident response Web site that provides information on incident response, including what to do if a user discovers a virus; suspicious e-mail; the deliberate or inadvertent release of sensitive, classified, or safeguards information; or missing IT equipment.

The agency uses a variety of tools to detect and respond to cyber security incidents, and the CSIRT conducts periodic incident response testing. The test results are documented and include a description of the scenario and responses to scenario questions on preparation; response and analysis; containment, eradication, and recovery; and forensics. The test results also include a checklist of actions that should have been taken during the exercise and documented lessons learned.

Based on our analysis, Carson Associates determined that the NRC incident response and reporting program includes the five attributes specified in the OMB requirement.

[13] CSIRT does not report incidents directly to law enforcement. If an incident might warrant reporting to law enforcement, CSIRT notifies the OIG Computer Crimes Unit, which then decides whether or not external law enforcement should be involved.

3.5 Status of Security Training Program (Question 5)

OMB Requirement	OIG Response
5a. The Agency has established and is maintaining a security training program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following six attributes: *1. Documented policies and procedures for security awareness training.* *2. Documented policies and procedures for specialized training for users with significant information security responsibilities.* *3. Appropriate training content based on the organization and roles.* *4. Identification and tracking of all employees with login privileges that need security awareness training.* *5. Identification and tracking of employees without login privileges that require security awareness training.* *6. Identification and tracking of all employees with significant information security responsibilities that require specialized training.*	X
5b. The Agency has established and is maintaining a security training program. However, the Agency needs to make significant improvements as noted below.	
5c. The Agency has not established a security training program.	

FISMA requires agencies to develop, document, and implement an agencywide information security program that includes security awareness training to information personnel, including contractors and other users of information systems that support the operations and assets of the agency. The security awareness training must inform personnel of information security risks associated with their activities; and their responsibilities in complying with agency policies and procedures designed to reduce these risks.

The NRC Security Training Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's security training program, Carson Associates reviewed the agency's policies, procedures, and guidance related to security training. To determine if the agency's security training program includes the six attributes specified in the OMB requirement, in addition to the agency's security training policies, procedures, and guidelines, we reviewed the annual security control test report for the agency's common controls. Security awareness training policies and procedures are provided at the agency level for all NRC information systems.

All new NRC employees (including onsite contractors, interns, and summer hires) are required to attend orientation the first day they report for duty. During the orientation, employees are given a brief presentation on a variety of NRC IT-related policies that includes a discussion on appropriate use of IT equipment. In addition, a representative from the Office of the General

Counsel presents a session on ethics that includes additional discussions on appropriate use of the Internet. In addition, all NRC computer users, including Federal employees, detailees, interns, and contractors, are required to take an annual online computer security awareness course.

The agency also routinely issues network announcements on various security topics, including hoax e-mail messages, phishing and spear phishing, spam, and the risks of using thumb drives. In the spring of 2009, NRC began publishing a quarterly IT security newsletter, FRONTLINE. The newsletters will provide the NRC with IT security awareness tips and techniques for protecting one's information.

For FY 2010, all NRC computer users, including Federal employees, detailees, interns, and contractors, were required to take an online computer security awareness course. All NRC employees and support contractors having network accounts were required to complete the course within 60 days of the course's availability, with a target cutoff date of August 3, 2010, for completion of the course. The self-paced course consisted of two modules – a general computer security awareness training module develop by another Government agency for governmentwide use, and an NRC-specific module tailored to address the IT protection of SGI and rules of behavior for all users of NRC computing resources. Completion of both modules was required to fulfill the annual computer security awareness training requirement. The agency also prepared a list of differences between NRC policy and the course content of the first module as a companion document to the FY 2010 training. Office training coordinators were required to track completion of the computer security awareness course and report weekly completion percentages to the CSO. In an announcement dated August 4, 2010, the agency reported 5,007 users had completed the FY 2010 computer security awareness course – the equivalent of 98 percent of NRC computer users. The CSO's IT Security Training Web site also includes a link to a Web page showing the completion rate for the computer security awareness training by office.

On May 28, 2010, the Chief Information Security Officer (CISO) issued a memorandum asking for support and action to ensure that all employees with significant IT security responsibilities are appropriately identified. The memorandum required recipients of the memorandum to report back to the CISO by June 11, 2010, on the names of employees within their organization that have an IT security role as part of their official duties.

The agency also developed an IT Role-Based Training Plan that states the requirement for training for those with significant IT responsibilities, the type of training expected for each role, and frequency of training per role. System owners are responsible for using the training plan procedures to address the training needs of personnel with IT roles. The training plan defines the following IT security roles with significant IT security responsibilities that require role-based training.

- IT executive.
- System owner.
- IT auditor.
- IT functional manager.

- IT senior approving official.
- IT functional management and operations personnel (including information systems security officers (ISSO), database administrator, network administrator system administrator, and IT manager).
- IT system development official.
- IT project officer.
- IT system developer.

NRC is pursuing three approaches to address IT role-based training: NRC-provided resident courses, use of ISS Line of Business (LoB) providers, and commercially provided training and certifications.

- **NRC-provided courses:** The agency already provides IT security awareness training courses for ISSOs and for system and network administrators. These courses must be taken upon appointment to the role and every 3 years thereafter. The agency now also requires IT managers and system owners to complete role-specific training every 3 years. Senior level managers and IT executive are also required to complete role-specific training every 3 years. The agency developed separate courses for personnel in these roles. The agency also developed a laptop security controls training course for ISSOs. This course provides training in how to configure laptops with required computer security controls and how to verify configuration of laptops' compliance with FDCC and NRC requirements.
- **ISS LoB Providers:** The CSO coordinated with the Department of Defense for the use of its ISS LoB approved courseware for agency-wide general computer security awareness.
- **Commercial Training:** The CSO IT Security Role-Based Training Web page provides lists of commercially available training in three areas: technical certification/courses, operating system-specific or database certifications/courses, and managerial/project management certification/courses. The Web page also provides a crosswalk between the 12 IT security roles and the commercially available training.

Based on our analysis, Carson Associates determined that the NRC security training program includes the six attributes specified in the OMB requirement.

3.6 Status of POA&M Program (Question 6)

OMB Requirement	OIG Response
6a. The Agency has established and is maintaining a POA&M program that is generally consistent with NIST's and OMB's FISMA requirements and tracks and monitors known information security weaknesses. Although improvement opportunities may have been identified by the OIG, the program includes the following six attributes: *1. Documented policies and procedures for managing all known IT security weaknesses.* *2. Tracks, prioritizes, and remediates weaknesses.* *3. Ensures remediation plans are effective for correcting weaknesses.* *4. Establishes and adheres to reasonable remediation dates.* *5. Ensures adequate resources are provided for correcting weaknesses.* *6. Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly.*	
6b. The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below.	X
6a(2) POA&M procedures are not fully developed, sufficiently detailed or consistently implemented.	X
6a(3) POA&Ms do not include all known security weaknesses (OMB M-04-25).	X
6a(8) Initial target remediation dates are frequently missed (OMB M-04-25).	X
6a(9) POA&Ms are not updated in a timely manner (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).	X
6c. The Agency has not established a POA&M program.	

FISMA requires agencies to develop, document, and implement an agencywide information security program that includes a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. MD and Handbook 12.5 requires system owners/sponsors to ensure that a POA&M is developed, implemented, and maintained to track the major weaknesses that have been identified for office-sponsored information systems. Each office is required to regularly update the CIO on its progress in correcting system weaknesses to enable the CIO to provide the agency's quarterly FISMA update report to OMB.

Agency POA&M Process – Background

NRC has two primary tools for tracking IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on

behalf of the agency. At a high level, NRC uses the POA&Ms required by OMB to track (1) corrective actions from the OIG annual independent evaluation; (2) corrective actions from the agency's annual review; and (3) recurring FISMA and IT security action items, such as annual security control assessments and annual contingency plan testing. The POA&Ms may also include corrective actions resulting from other security studies conducted by or on behalf of NRC.

The more specific corrective actions associated with the certification and accreditation process (e.g., corrective actions resulting from risk assessments and security control testing) are tracked in Rational® ClearQuest®[14] as change requests using the PMM process for change management. All certification and accreditation corrective actions arising from the security control testing process and from vulnerability scans are imported into Rational ClearQuest. A corrective action plan is generated directly from Rational ClearQuest. System owners are responsible for remediation of each corrective action within the timeframes specified in the corrective action plan using the PMM process for change requests.

The agency developed a process for requesting quarterly POA&M updates from system owners, compiling the data into a consolidated source, reviewing it for accuracy, rolling up the information, and reporting it to OMB. Five weeks prior to the quarterly submittal to OMB, the agency sends out a data call to the offices asking them to update the current POA&Ms for their systems and add new weaknesses to the POA&Ms. Three weeks prior to the quarterly submittal to OMB, the agency receives the updated POA&M data from the system owners and enters the data into NSICD. The agency adds any new weaknesses identified from various sources, including OIG audits and reports, Government Accountability Office audits, internal control reviews, annual security control testing, security test and evaluation, information security program reviews, critical infrastructure protection vulnerability assessments, risk assessments, penetration tests, security information assessment recommendations, security assessment reports, quarterly scanning, vulnerability assessment reports, and confirmed security incidents. The agency provides instructions on providing the quarterly updates to the POA&Ms and specifies that data in only four fields on the POA&Ms should be changed: resources, brief description of work/services required, changes to milestones, and status.

The FY 2007, FY 2008, and FY 2009 FISMA independent evaluations found that the quality of the agency's POA&Ms needed improvement. Specifically, Carson Associates found that (1) the metrics submitted to OMB often deviated from the actual POA&Ms, (2) the agency did not always follow OMB and internal NRC POA&M guidance, (3) POA&Ms do not include all known security weaknesses, (4) deficiencies were not always remediated in a timely manner, (5) estimated dates for remediation were not always adhered to, and (6) the agency was closing weaknesses without sufficient evidence from the system owner.

As a result of recommendations from the FY 2007 FISMA independent evaluation, the agency has been working on automating the POA&M process and is currently using NSICD to store, process, and generate the POA&Ms. In 2008, the agency acquired the Environmental Protection Agency's FISMA reporting solution, the Automated System Security Evaluation and Remediation Tracking system, to further automate the POA&M and continuous monitoring

[14] Rational ClearQuest is an IBM software package used for software change management.

processes. However, the agency identified some problems with the tool, and after 6 months of research and evaluation, the CSO picked Xacta, which was purchased in the second half of 2009, as the agency's tool for automating the POA&Ms. As of the completion of fieldwork, the agency had not begun using Xacta for automating the POA&Ms.

The agency also issued CSO-PROS-2016, NRC POA&M Process, V1.7, to ensure quality assurance is emphasized. The document includes a process for conducting independent verification and validation of POA&Ms to assure their adequacy as part of the security assessment review process. Additionally, CSO acquired additional contract support to assist in establishing a compliance review process in which CSO will review security documentation, conduct vulnerability scanning, and meet with each system owner on an annual basis to verify the status of remediation efforts, assess the comprehensiveness of planned corrective actions, and validate the accuracy of tasks, responsibilities, and milestones for each outstanding weakness. These activities take place quarterly, targeting approximately 25 percent of the overall number of POA&Ms. The first POA&M scoring notifications were issued in the 2nd quarter of FY 2010. The POA&M process was also briefed to various system owners and internal forums.

The agency's new POA&M procedures also require corrective actions to be ranked based upon the most critical security weaknesses and their impact on the agency's mission. This ranking should be reflected in the POA&Ms by listing identified weaknesses in priority order, irrespective of the weakness identifier (which is sequentially derived). The procedures state that the overall severity of the weakness should be considered in conjunction with the system risk impact level when prioritizing the mitigation of weaknesses. Weakness severity is the potential magnitude of loss that could result from weakness exploitation. The POA&Ms includes a weakness severity (called risk level) column that can be used to prioritize security weaknesses. However, the agency has not implemented the process described above for prioritizing security weaknesses.

FINDING – The Agency's POA&M Program Still Needs Improvement (Repeat Finding)

Despite the issuance of the new NRC POA&M Process, the implementation of the POA&M scoring, and the briefing of the POA&M process to various system owners and internal forums, the agency's POA&M program still needs improvement. This is primarily due to the manual process still in use for managing and updating the POA&Ms.

The agency's POA&M program may include some of the six attributes specified in the OMB requirement; however, as in previous independent evaluations, Carson Associates found that the quality of the agency's POA&Ms is not improving. In assessing the agency's POA&M program, Carson Associates found that (1) POA&M procedures are not fully developed, sufficiently detailed, or consistently implemented; (2) POA&Ms do not include all known security weaknesses; (3) initial target remediation dates are frequently missed; and (4) POA&Ms are not updated in a timely manner.

(1) POA&M Procedures Are Not Fully Developed, Sufficiently Detailed, or Consistently Implemented

As in previous independent evaluations, Carson Associates found that the following problems with POA&M procedures still persist: (1) the metrics submitted to OMB often deviated from the actual POA&Ms, (2) the agency is not always following OMB and internal NRC POA&M guidance, and (3) the agency is closing weaknesses without sufficient evidence from the system owners.

- **Metrics Submitted to OMB Deviate From the Actual POA&Ms:** As in previous independent evaluations, Carson Associates found discrepancies between the metrics submitted to OMB and the actual POA&Ms. The most common errors causing the discrepancies are:

  - Counting weaknesses as closed in more than one quarter.
  - Counting weaknesses as closed when they have not been closed by the OIG.
  - Reporting weaknesses as on track when they are actually delayed.
  - Reporting weaknesses as delayed when they are still on track.

- **The Agency Is Not Always Following OMB and NRC Internal POA&M Guidance:** As in previous FISMA evaluations, Carson Associates also found that the agency is not always following OMB's POA&M guidance. The agency is also not following NRC internal POA&M guidance. The following are some examples of deviations from OMB and NRC internal POA&M guidance found on the POA&Ms that were analyzed.

  - Weaknesses with completion dates over a year old are not always removed from the POA&Ms. OMB guidance[15] states that weaknesses that are no longer undergoing correction and have been completely mitigated for over a year should no longer be reported in the agency POA&Ms.
  - Weaknesses with changes made to scheduled completion dates. OMB guidance states that once an agency has completed the initial POA&M, no changes should be made to the scheduled completion date.
  - Weaknesses without scheduled completion dates. Several items added to the POA&Ms did not have scheduled completion dates.
  - Weaknesses not properly marked to indicate they were closed in a previous quarter, but are being reported as closed in a later quarter (NRC requirement).

- **The Agency Continues To Close Weaknesses Without Sufficient Evidence from the System Owners:** As in the FY 2008 and FY 2009 FISMA independent evaluations, Carson Associates found that the agency is sometimes closing weaknesses without sufficient evidence from the system owners. During our analysis of weaknesses identified during the FY 2010 annual security control testing, we found many instances

[15] OMB Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*.

where weaknesses that had been previously closed were still found to be present. In some instances, the weaknesses were added back to the POA&Ms with the FY 2010 annual security control testing results.

(2) POA&Ms Do Not Include All Known Security Weaknesses

The POA&M process is an agencywide process, but the POA&Ms do not include all known security weaknesses. For example, the POA&Ms do not include all weaknesses identified in OIG audits. The new agency POA&M procedures require new weaknesses to be added to the POA&Ms within 15 days of discovery. However, weaknesses from one of the regional reviews conducted in FY 2009 were not added to the POA&Ms until more than 3 months after the reports were issued. In addition, not all the weaknesses from the FY 2009 regional reviews were added to the POA&Ms. One report had eight weaknesses, but only four were added to the POA&Ms. Another report had 10 weaknesses, but only 7 were added to the POA&Ms. A third report had six weaknesses, but only five were added to the POA&Ms. Carson Associates also determined that none of the recommendations from the FY 2010 contingency plan testing, and not all of the weaknesses identified during the FY 2010 annual security control testing, have been added to the POA&Ms.

(3) Initial Target Remediation Dates Are Frequently Missed

Carson Associates analyzed the POA&Ms for the four systems selected for evaluation in FY 2010 in order to determine if target remediation dates are met. Three of the four systems had at least one weakness that was closed between 5 and 8 months after the scheduled completion date. One system had 3 weaknesses that were closed over a year after their scheduled completion dates. Two of the four systems have more than half of their open weaknesses overdue. One system has more than half of its open weaknesses overdue by more than 1 year.

(4) POA&Ms Are Not Updated in a Timely Manner

Carson Associates analyzed all of the agency's FY 2010 POA&M submissions to OMB to determine whether POA&Ms are updated in a timely manner. We found multiple instances of POA&M items being reported closed more than 3 months after they were actually closed. For example, there were more than 100 POA&M items reported closed at least 1 quarter after they were actually closed. In addition, we found multiple instances of the agency not counting weaknesses as closed when they had been closed by the OIG prior to the cutoff date for POA&M reporting.

RECOMMENDATIONS

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

1. Implement an automated tool to ensure the agency's POA&M procedures are consistently implemented.
2. Perform more frequent independent verification and validation of POA&Ms to ensure POA&Ms include all known security weaknesses, including those identified in OIG

audits, contingency plan testing, and annual security control testing, and to ensure POA&Ms are updated in a timely manner.

NRC Progress in Correcting Weaknesses Reported on Its POA&Ms Is Improving

The agency progress in correcting weaknesses reported on its POA&Ms is improving. In FY 2008 (quarters 1, 2, and 3), the agency closed just over 45 percent of its program level weaknesses and just over 43 percent of its system level weaknesses, which was somewhat of an improvement over FY 2007. However, in FY 2009 (FY 2008 4th quarter, and all quarters of FY 2009), the agency closed only 30 percent of its program level weaknesses and just over 40 percent of its system level weaknesses, which is less than in FY 2008. In FY 2010, the agency closed just over 46 percent of its program level weaknesses and just over 68 percent of its system level weaknesses, which is an improvement over FY 2009.

3.7 Status of Remote Access Program (Question 7)

OMB Requirement	OIG Response
7a. The Agency has established and is maintaining a remote access program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following seven attributes: *1. Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access.* *2. Protects against unauthorized connections or subversion of authorized connections.* *3. Users are uniquely identified and authenticated for all access.* *4. If applicable, multi-factor authentication is required for remote access.* *5. Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms.* *6. Requires encrypting sensitive files transmitted across public networks or stored on mobile devices and removable media such as CDs and flash drives.* *7. Remote access sessions are timed-out after a maximum of 30 minutes of inactivity after which re-authentication is required.*	X
7b. The Agency has established and is maintaining a remote access program. However, the Agency needs to make significant improvements as noted below.	
7c. The Agency has not established a program for providing secure remote access.	

On June 26, 2008, the agency issued the NRC Computer Security Information Protection Policy to address requirements specified OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, and M-06-19, *Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency IT Investments*. The policy includes the requirement for remote access to any

system that processes non-public NRC information to be constrained by a "time-out" function that requires re-authentication after 30 minutes of inactivity.

In December 2008, the agency issued a computer security policy for encryption of data at rest prior to removal from agency facilities, and updated NUREG/BR-168, Guide for IT Security, Policy for Processing Unclassified Safeguards Information on NRC Computers. This policy requires the use of encryption to protect sensitive data at rest, including when stored on media such as CDs, DVDs, thumb drives, backups, and external hard drives. The policy also states that the agency will be issuing a separate policy to address encryption of transmitted data.

On May 21, 2009, the agency issued the NRC Agencywide Rules of Behavior for Authorized Computer Use. The rules of behavior are provided to NRC computer users as part of the annual computer security awareness training course, and apply to all NRC employees, contractors, vendors, and agents (users) who have access to any system operated by the NRC or by a contractor or outside entity on behalf of the NRC. The rules of behavior include a requirement for users to use only NRC-approved technologies for remote access to the NRC network.

The NRC Remote Access Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's remote access program, Carson Associates reviewed the agency's policies, procedures and guidance related to remote access. To determine if the agency's remote access program includes the seven attributes specified in the OMB requirement, in addition to the agency's remote access policies, procedures, and guidelines, we reviewed the annual security control test report for the agency's common controls and the security test and evaluation results for the four systems selected for evaluation in FY 2010, specifically the test results for the AC-17 control, Remote Access. This control requires organizations to authorize, monitor, and control all methods of remote access to their information systems.

NRC provides centralized remote access via a component of its IT infrastructure system. After remote access through the centralized component, users have the same access to the network, NRC information, and NRC information systems as if they were logged into the network locally. The agency monitors remote access via a variety of mechanisms. At the common control level, this control was found to be in place. Of the four systems reviewed, this control was in place for one system (provided by the agency's IT infrastructure system), partially in place for one system, planned for one system, and not applicable for one system. The agency is in the process of procuring modems with Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*, validated cryptographic capabilities for one system and has determined that there are compensating controls in place for the other system in which this control was identified as inadequate.

Based on our analysis, Carson Associates determined that the NRC remote access program includes the seven attributes specified in the OMB requirement.

3.8 Status of Account and Identity Management Program (Question 8)

OMB Requirement	OIG Response
8a. The Agency has established and is maintaining an account and identity management program that is generally consistent with NIST's and OMB's FISMA requirements and identifies users and network devices. Although improvement opportunities may have been identified by the OIG, the program includes the following seven attributes: *1. Documented policies and procedures for account and identity management.* *2. Identifies all users, including federal employees, contractors, and others who access Agency systems.* *3. Identifies when special access requirements (e.g., multi-factor authentication) are necessary.* *4. If multi-factor authentication is in use, it is linked to the Agency's personal identity verification program.* *5. Ensures that the users are granted access based on needs and separation of duties principles.* *6. Identifies devices that are attached to the network and distinguishes these devices from users.* *7. Ensures that accounts are terminated or deactivated once access is no longer required.*	X
8b. The Agency has established and is maintaining an account and identity management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.	
8c. The Agency has not established an account and identity management program.	

MD and Handbook 12.5, Appendix A, Section 2.1, provides an agencywide identification and authentication policy for all systems. System owners may develop a system-specific identification and authentication policy to address system-specific requirements. System owners are responsible for developing, disseminating, reviewing, and updating formal, documented system-specific procedures to facilitate policy-compliant implementation of the identification and authentication policy and associated controls.

The NRC Account and Identity Management Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's account and identity management program, Carson Associates reviewed the agency's policies, procedures and guidance related to account and identity management. To determine if the agency's account and identity management program includes the seven attributes specified in the OMB requirement, in addition to the agency's remote access policies, procedures, and guidelines, we reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2010. Test results for the following controls related to account and identity management were reviewed:

- AC-2, Account Management – Requires organizations to manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts, and to review system accounts at least annually.
- IA-2, User Identification and Authentication – Requires information systems to uniquely identify and authenticate users (or processes acting on behalf of users). Also specifies requirements for the use of multi-factor authentication.
- IA-3, Device Identification and Authentication – Requires information systems to identify and authenticate specific devices before establishing a connection.
- IA-4, Identifier Management – Requires organizations to manage user identifiers by (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official; (iv) issuing the user identifier to the intended party; (v) disabling the user identifier after an organization-defined period of inactivity; and (vi) archiving user identifiers.

We also reviewed the annual security control test report for the agency's common controls, specifically for control IA-1, Identification and Authentication Policy and Procedures. This control requires organizations to develop, disseminate, and periodically review/update (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls. The testing found that the agency has developed and disseminated an agencywide identification and authentication policy for all systems; however, periodic reviews and updates of the identification and authentication policy and procedures within MD and Handbook 12.5 have not been accomplished. MD and Handbook 12.5 is currently undergoing an update. In addition, the testing found that the identification and authentication policy does not sufficiently address purpose, scope, roles and responsibilities, management commitment, coordination among organizational entities, and compliance.

Of the four systems reviewed, these controls were not applicable for one system. One or more of these controls were found to be not in place for the other three systems. Specific issues included problems with granting access without proper authorization, reviewing accounts, disabling inactive accounts, and auditing account management actions. The agency has corrected some of the identified deficiencies and is in the process of correcting the remaining items. Testing also identified issues with the use of multi-factor authentication for certain types of access. Resolution of this issue is dependent on completion of the agency's implementation of the HSPD-12 personal identity verification card.

Based on our analysis, Carson Associates determined that the NRC account and identity management program includes the seven attributes specified in the OMB requirement.

3.9 Status of Continuous Monitoring Program (Question 9)

OMB Requirement	OIG Response
9a. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following four attributes: *1. Documented policies and procedures for continuous monitoring.* *2. Documented strategy and plans for continuous monitoring, such as vulnerability scanning, log monitoring, notification of unauthorized devices, sensitive new accounts, etc.* *3. Ongoing assessments of selected security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.* *4. Provides system authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions.*	X
9b. The Agency has established an entity-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.	
9c. The Agency has not established a continuous monitoring program.	

FISMA requires agencies to develop, document, and implement an agencywide information security program that includes periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. Such testing shall include testing of management, operational, and technical controls of every information system identified in the inventory required by FISMA.

NIST SP 800-53 requires organizations to establish a continuous monitoring strategy and implement a continuous monitoring program that includes (i) a configuration management process for the information system and its constituent components, (ii) a determination of the security impact of changes to the information system and environment of operation, (iii) ongoing security control assessments in accordance with the organizational continuous monitoring strategy, and (iv) reporting the security state of the information system to appropriate organizational officials at a frequency to be determined by the organization.

The NRC Continuous Monitoring Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's continuous monitoring program, Carson Associates reviewed the agency's policies, procedures, and guidance related to continuous monitoring. To determine if the agency's continuous monitoring program includes the four attributes specified in the OMB requirement, in addition to the agency's continuous monitoring policies, procedures, and

guidelines, we reviewed the continuous monitoring activities performed for all of the agency's operational systems, including contractor systems.

The agency Executive Director for Operations issued a memorandum in January 2010 requiring system owners to perform continuous monitoring activities required for FISMA. System owners were required to take the following actions:

1. Prepare a schedule of planned contingency plan testing and annual security controls testing, with a completion date that does not exceed 1 year from the last time such testing was performed.
2. Submit an updated contingency plan test plan and contingency plan test report to CSO.
3. Perform annual security testing and ensure that all annual security control testing reports are submitted in a timely fashion.
4. For systems owned and/or operated by other agencies or contractors, obtain a memorandum from the owning/operating agency/contractor stating that annual contingency plan and security control testing has been performed in accordance with FISMA and NRC instructions, and submit the memorandum to CSO by July 30, 2010.
5. If applicable, reauthorize systems in accordance with FISMA and NRC requirements.
6. Update all security-related documentation in accordance with FISMA and NRC requirements.
7. Proactively track and mitigate POA&M weaknesses identified during the course of ongoing security activities and submit a POA&M transmittal memorandum each quarter to CSO.

Systems that were authorized to operate within the past fiscal year already had their security controls tested and, therefore, did not require additional annual security control testing. The CSO identified a set of 96 core controls that must be assessed annually for all systems. System owners were required to select additional controls with an emphasis on controls associated with POA&M items that have been closed within the past year, and with additional controls selected by the authority of the system owner and controls added by Revision 3 of NIST SP 800-53.

The agency also issued CSO-PROS-1323, US NRC Agency-wide Continuous Monitoring Program, in June 2010. This document provides direction for NRC continuous monitoring activities and describes the process for annual continuous monitoring reviews, related roles and responsibilities and evaluation criteria. Continuous monitoring reviews are conducted on each office and their respective systems once per fiscal year to provide system owners and the designed approving authorities with insight into the agencywide IT security posture.

Contingency plan testing is discussed in Section 3.10. Procedures for the oversight of contractor systems are discussed in Section 3.11. The agency's certification and accreditation program is discussed in Section 3.2. The agency's POA&M program is discussed in Section 3.6. Annual security control testing and security plan updates are discussed below.

Carson Associates determined that the NRC continuous monitoring program includes the four attributes specified in the OMB requirement.

NRC Has Completed Annual Security Control Testing for All Agency Systems and for All Contractor Systems

Six of the agency's 25 operational systems and 1 of the agency's 3 contractor systems were authorized to operate in the past fiscal year and, therefore, did not require additional annual security control testing. The remaining 19 agency systems and 2 contractor systems required annual security control testing. As of the completion of fieldwork for FY 2010, annual security control testing was completed for the 19 agency systems and 2 contractor systems that required such testing.

Table 3-3. Total Number of Systems and Number Reviewed for Which Security Controls Have Been Tested and Reviewed in the Past Year by FIPS 199 System Impact Level

FIPS 199 System Impact Level	Agency	Contractor	Total Number	Number Reviewed
High	9	1	10	2
Moderate	16	1	17	2
Low	0	1	1	0
Not Categorized	0	0	0	0
Total	25	3	28	4

NRC Has Updated Security Plans for All Agency Systems and for All Contractor Systems

As of the completion of fieldwork for FY 2010, all 25 agency systems, and all 3 contractor systems for which NRC has direct oversight had new or updated security plans.

3.10 Status of Contingency Planning Program (Question 10)

OMB Requirement	OIG Response
10a. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program that is generally consistent with NIST's and OMB's FISMA requirements. Although improvement opportunities may have been identified by the OIG, the program includes the following seven attributes: *1. Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster.* *2. The agency has performed an overall Business Impact Assessment.* *3. Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures.* *4. Testing of system specific contingency plans.* *5. The documented business continuity and disaster recovery plans are ready for implementation.* *6. Development of training, testing, and exercises (TT&E) approaches.* *7. Performance of regular ongoing testing or exercising of continuity/disaster recovery plans to determine effectiveness and to maintain current plans.*	X
10b. The Agency has established and is maintaining an entity-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.	
10c. The Agency has not established a business continuity/disaster recovery program.	

FISMA requires agencies to develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. 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(es), or the contingency plan. MD and Handbook 12.5 states that the NRC shall comply with the NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, IT risk assessments, and IT contingency plans) and other applicable NIST automated information security guidance for IT security processes, procedures, and testing. MD and Handbook 12.5 also states that IT contingency plans for major applications and general support systems shall be tested each year. A live test provides the best indication of the adequacy of a contingency plan test. If a live test cannot be conducted due to operational constraints, a simulated test may be conducted in lieu of the live test. NRC CSO and OIS procedures also require annual contingency plan testing for all major applications and general support systems, including generating a contingency plan test report.

The NRC Contingency Planning Program Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's contingency planning program, Carson Associates reviewed the agency's policies, procedures and guidance related to contingency planning. To determine if the agency's contingency planning program includes the seven attributes specified in the OMB requirement, in addition to the agency's contingency planning policies, procedures, and guidelines, we reviewed the contingency plans and contingency plan test reports for all of the agency's operational systems, including contractor systems.

In early 2009, the agency conducted a business impact analysis in support of the development of the NRC Disaster Recovery Plan. The purpose of the analysis was to collect information from each office to document business processes along with other relevant information supporting the agency's mission. In the near term, this data will be used to form the basis for prioritization of "business critical" IT systems currently in use at the NRC to determine systems to be covered under the disaster recovery plan. This information will also be used in the development of long term funding needs to support the disaster recovery solution for the NRC.

Carson Associates determined that the NRC contingency planning program includes the seven attributes specified in the OMB requirement.

Annual Contingency Plan Testing Was Completed for Almost All Agency Systems and All Contractor Systems

The Executive Director for Operations issued a memorandum in January 2010 requiring system owners to perform continuous monitoring activities required for FISMA, including completing annual contingency plan testing of all major applications and general support systems. System owners were required to prepare a schedule of planned contingency plan testing with a completion date that does not exceed 1 year from the last time such testing was performed.

As of the completion of fieldwork for FY 2010, contingency plan testing[16] was completed for 24 of the agency's 25 operational information systems and for all 3 contractor systems for which NRC has direct oversight. The one system for which contingency plan testing has not yet occurred is a new system that just went into production in early 2010. This system is undergoing a scope change resulting in a delay in developing and testing the contingency plan. In addition, 24 of the agency's 25 operational NRC information systems and all 3 contractor systems have current contingency plans. It should be noted that the contingency plan for one of the agency's operational systems was not updated until after the September 30, 2010 cutoff date for reporting completion metrics. It should also be noted that in its 4th quarter FISMA metrics, the agency reported 100 percent of their systems had contingency plans tested in accordance with policy, when in fact; one system has not had its contingency plan tested.

[16] Any testing performed between October 1, 2009, and the completion of fieldwork would be considered as FY 2010 test results.

Table 3-4. Total Number of Systems and Number Reviewed for Which Contingency Plans Have Been Tested in Accordance With Policy by FIPS 199 System Impact Level

FIPS 199 System Impact Level	Agency	Contractor	Total Number	Number Reviewed
High	9	1	10	2
Moderate	15	1	16	2
Low	0	1	1	0
Not Categorized	0	0	0	0
Total	24	3	27	4

3.11 Status of Agency Program To Oversee Contractor Systems (Question 11)

OMB Requirement	OIG Response
11a. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. Although improvement opportunities may have been identified by the OIG, the program includes the following six attributes: 1. *Documented policies and procedures for information security oversight of systems operated on the Agency's behalf by contractors or other entities the Agency obtains sufficient assurance that security controls of systems operated by contractors or others on its behalf are effectively implemented and comply with federal and agency guidelines.* 2. *A complete inventory of systems operated on the Agency's behalf by contractors or other entities.* 3. *The inventory identifies interfaces between these systems and Agency-operated systems.* 4. *The agency requires agreements (MOUs, Interconnect Service Agreements, contracts, etc.) for interfaces between these systems and those that is owns and operates.* 5. *The inventory, including interfaces, is updated at least annually.* 6. *Systems that are owned or operated by contractors or entities are subject to and generally meet NIST and OMB's FISMA requirements.*	X
11b. The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities. However, the Agency needs to make significant improvements as noted below.	
11c. The Agency does not have a program to oversee systems operated on its behalf by contractors or other entities.	

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 or (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[17]

NRC defines two types of systems that are operated by a contractor or other organization on behalf of NRC – contractor systems and e-Government systems. A contractor system is a system that processes NRC information and is operated and maintained by a contractor, and an e-Government system is a system that processes NRC information and is operated and maintained by another Federal agency.

The agency follows the same policies, procedures, and guidance in MD and Handbook 12.5 for contractor systems as it does for agency systems. All contractor systems must be certified and accredited prior to processing any sensitive NRC information or connecting to the NRC infrastructure and must undergo annual security control testing and annual contingency plan testing. Contractor systems are also required to undergo recertification and reaccreditation per NRC policy.

For e-Government systems, the agency requires the responsible NRC system owner to demonstrate those systems meet FISMA requirements by providing proof of authority to operate, annual security control testing, and annual contingency plan testing. The agency also requires a privacy impact assessment and a security categorization for all e-Government systems. The agency may also require service level agreements or memoranda of understanding/agreement with those agencies.

In addition to three contractor systems, NRC has eight e-Government systems, all considered to be major applications. Oversight of these systems is the responsibility of the Federal agencies operating the systems.

The NRC Program To Oversee Contractor Systems Is Generally Consistent with NIST's and OMB's FISMA Requirements

In order to evaluate the agency's program to oversee contractor systems, Carson Associates reviewed the agency's policies, procedures and guidance related to contractor oversight. To determine if the agency's program to oversee contractor systems includes the six attributes specified in the OMB requirement, in addition to the agency's contractor oversight policies, procedures, and guidelines, we reviewed the agency's inventory of systems; agreements such as MOUs, interconnection service agreements, and contracts; and annual security control test reports, certification and accreditation documents, and contingency plans and contingency plan test reports for the three contractor systems for which NRC has direct oversight.

We also reviewed proof of authority to operate, annual security control testing, and annual contingency plan testing for the eight e-Government systems, as well as the required privacy impact assessments and security categorizations.

[17] 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.

Carson Associates determined that the NRC contractor oversight program includes the six attributes specified in the OMB requirement.

Agency Oversight of Contractor Systems Meets FISMA Requirements

As of the completion of fieldwork for FY 2010, all three contractor systems for which NRC has direct oversight had a current certification and accreditation. One was authorized to operate in FY 2010 and did not require additional annual security control testing. The other two had their security controls tested and reviewed in the past year. All three have completed annual contingency plan testing.

[Page intentionally left blank]

4 Consolidated List of Recommendations

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

1. Implement an automated tool to ensure the agency's POA&M procedures are consistently implemented.
2. Perform more frequent independent verification and validation of POA&Ms to ensure POA&Ms include all known security weaknesses, including those identified in OIG audits, contingency plan testing, and annual security control testing, and to ensure POA&Ms are updated in a timely manner.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on November 5, 2010, agency officials agreed with the report's findings and recommendations and provided some editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[Page intentionally left blank]

Appendix. SCOPE AND METHODOLOGY

Carson Associates performed an independent evaluation of NRC's Implementation of FISMA for FY 2010. To conduct the independent evaluation, the team met with agency staff responsible for implementing the agency's information system security program, reviewed certification and accreditation documentation for the agency's operational information systems, and reviewed other documentation provided by the agency that demonstrated its implementation of FISMA.

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

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

This work was conducted between April 2010 and September 2010. 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; Joe Rood, CISSP, CISA; John Braden, CISSP; and Edwin Caron, CISA, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]