EVALUATION REPORT

Independent Evaluation of NRC's
Implementation of the Federal
Information Security Management
Act for Fiscal Year 2009

OIG-10-A-04 November 17, 2009

OFFICE OF THE INSPECTOR GENERAL
U.S. NUCLEAR REGULATORY COMMISSION

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

OFFICE OF THE
INSPECTOR GENERAL

November 17, 2009

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 FOR FISCAL YEAR 2009 (OIG-10-A-04)

Attached is the Office of the Inspector General's (OIG) independent evaluation report titled, *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2009 (OIG-10-A-04).*

The report presents the results of the subject audit. Agency comments provided during an October 30, 2009, exit conference have been incorporated, as appropriate, into this report.

Please provide information on actions taken or planned on the recommendation 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 audit. 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, Jr., Director, Office of Commission Appellate Adjudication
James E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
R. William Borchardt, Executive Director for Operations
Bruce S. Mallett, Deputy Executive Director for Reactor
  and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research,
  State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Corporate Management
  and Chief Information Officer, OEDO
Nader L. Mamish, Assistant for Operations, OEDO
Kathryn O. Greene, Director, Office of Administration
Patrick D. Howard, Director, Computer Security Officer
Roy P. Zimmerman, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
  and Environmental Management Programs
Cheryl A. 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
Michael F. Weber, 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
Samuel J. Collins, 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

Carson

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2009

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

November 6, 2009

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

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine 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-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009, requires the agency's IG to report their responses to OMB's annual FISMA reporting questions for IGs via an automated collection tool.

Richard S. Carson and Associates, Inc. (Carson Associates), performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2009. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for IGs 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, 2009.

PURPOSE

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2009.

RESULTS IN BRIEF

Program Enhancements and Improvements

Over the past 7 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. In 2007, the Commission approved the establishment of the Computer Security Office. The new office reports to the Deputy Executive Director for Corporate Management and Chief Information Officer (CIO) and is headed by the Chief Information Security Officer (CISO). The CISO plans, directs, and oversees the implementation of a comprehensive, coordinated, integrated, and cost-effective NRC information technology (IT) security program, consistent with

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

applicable laws; regulations; Commission, Executive Director for Operations, and CIO direction; management initiatives; and policies.

The agency has accomplished the following since the FY 2008 FISMA independent evaluation:

- The agency made significant progress in certifying and accrediting its systems. In FY 2009, the agency completed certification and accreditation of 12 of the agency's 22 operational systems and 1 of the agency's 3 contractor systems. As of the completion of fieldwork for FY 2009, all but one of the operational NRC information systems had a current certification and accreditation, and all three of the 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 19 of the agency's 22 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 agency systems and for all contractor systems.
- The agency issued several new and updated policies related to the protection of personally identifiable information (PII) including an updated *Computer Security Incident Response Policy*, an updated *PII Breach Notification Policy*, an updated *Computer Security Information Protection Policy*, the *Laptop Security Policy,* and the *Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities*.
- The agency issued the *Agency-wide 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 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 agency developed configuration guidance, configuration standards, and standard system security plans for laptops, as well as a new *Laptop Security Policy*.
- The agency identified all employees with significant IT security responsibilities and developed a plan for ensuring those employees receive appropriate role-based training.

Program Weaknesses

While the agency has made significant improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified two information system security program weaknesses. One is a repeat finding from the FY 2008 independent evaluation, and the other is a repeat finding from several previous independent evaluations.

- The NRC inventory interface information is still inconsistent (repeat finding).
- The quality of the agency's plans of action and milestones still needs improvement (repeat finding).

RECOMMENDATION

This report makes one new recommendation to further address the repeat finding concerning the interface information issue. Other recommendations for the repeat findings were made in previous reports.

AGENCY COMMENTS

At an exit conference on October 30, 2009, agency officials agreed with the report's findings and recommendation and provided a few editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

BPIAD	Business Process Improvement and Applications Division
Carson Associates	Richard S. Carson and 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
IAS	Information Assurance System
IATO	Interim Authorization to Operate
IG	Inspector General
IRSD	Information and Records Services Division
ISA	Interconnection Security Agreement
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
P2P	Peer-to-Peer
PIA	Privacy Impact Assessment
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
SSN	Social Security Number
SUNSI	Sensitive Unclassified Non-Safeguards Information
US-CERT	United States Computer Emergency Readiness Team

TABLE OF CONTENTS

List of Tables

1 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.[2] FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program and practices to determine 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-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009, requires the agency's IG to report their responses to OMB's annual FISMA reporting questions for IGs via an automated collection tool.

Richard S. Carson and Associates, Inc. (Carson Associates), performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2009. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for IGs 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, 2009.

2 Purpose

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2009. The Appendix contains a description of the evaluation scope and methodology.

3 Findings

Over the past 7 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. In 2007, the Commission approved the establishment of the Computer Security Office (CSO). The new office reports to the Deputy Executive Director for Corporate Management and Chief Information Officer (CIO) and is headed by the Chief Information Security Officer (CISO). The CISO plans, directs, and oversees the implementation of a comprehensive, coordinated, integrated, and cost-effective NRC information technology (IT) security program, consistent with applicable laws; regulations; Commission, Executive Director for Operations, and CIO direction; management initiatives; and policies.

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

The CSO was established to serve as the focal point for IT security and to provide vision, leadership, and oversight in developing, promulgating, and implementing an end-to-end NRC IT security strategy. The CSO is divided into three core areas: Cyber Situational Awareness, Analysis, and Response Team; FISMA Compliance and Oversight Team; and Policy, Standards, and Training Team. The CSO provides IT security oversight responsibility, coordinates the overall agency IT security program, develops policies and procedures, and provides assistance with security reviews, assessments, and plans to those offices requiring it.

The agency has accomplished the following since the FY 2008 FISMA independent evaluation:

- The agency made significant progress in certifying and accrediting its systems. In FY 2009, the agency completed certification and accreditation of 12 of the agency's 22 operational systems and 1 of the agency's 3 contractor systems. As of the completion of fieldwork for FY 2009, all but one of the operational NRC information systems had a current certification and accreditation, and all three of the 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 19 of the agency's 22 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 agency systems and for all contractor systems.
- The agency issued several new and updated policies related to the protection of personally identifiable information (PII) including an updated *Computer Security Incident Response Policy*, an updated *PII Breach Notification Policy*, an updated *Computer Security Information Protection Policy*, the *Laptop Security Policy*, and the *Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities*.
- The agency issued the *Agency-wide 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 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 agency developed configuration guidance, configuration standards, and standard system security plans for laptops, as well as a new *Laptop Security Policy*.
- The agency identified all employees with significant IT security responsibilities and developed a plan for ensuring those employees receive appropriate role-based training.

While the agency has made significant improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified two information system security program weaknesses. One is a repeat finding from the FY 2008 independent evaluation, and the other is a repeat finding from several previous independent evaluations.

- The NRC inventory interface information is still inconsistent (repeat finding).
- The quality of the agency's plans of action and milestones (POA&M) still needs improvement (repeat finding).

This report makes one new recommendation to further address the repeat finding concerning the interface information issue. Other recommendations for the repeat findings were made in previous reports.

The following sections present the detailed findings from the independent evaluation and are organized based on the IG section of the OMB FISMA reporting tool. Each major section corresponds to a question or set of questions from the template. Findings are presented in the sections to which they are relevant.

3.1 FISMA Systems Inventory (Question 1)

OMB Requirement	OIG Response
1. Identify the number of Agency and Contractor systems reviewed by component and FIPS 199 system impact level (low, moderate, high).	*See Table 3-1 below.*

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	8	2	1	0	9	2
Moderate	14	1	1	1	15	2
Low	0	0	1	0	1	0
Not Categorized	0	0	0	0	0	0
Total	22	3	3	1	25	4

As of completion of fieldwork, NRC has 22 operational systems that fall under FISMA reporting requirements.[3] Of the 22, 8 are general support systems,[4] and 14 are major applications.[5] NRC

[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.

has 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 2009 FISMA independent evaluation.

3.2 Certification and Accreditation (Question 2a)

OMB Requirement	OIG Response
2.a. Number of systems reviewed that are certified and accredited (certification and accreditation must be current) by FIPS 199 system impact level.	*See Table 3-2 below.*

Table 3-2. Total Number of Systems and Number Reviewed That Are Certified and Accredited by FIPS 199 System Impact Level[6]

FIPS 199 System Impact Level	Agency	Contractor	Total Number	Number Reviewed
High	8	1	9	2
Moderate	13	1	14	2
Low	0	1	1	0
Not Categorized	0	0	0	0
Total	21	3	24	4

NRC Has Made Significant Progress in Certifying and Accrediting Its Systems

The FY 2005, FY 2006, and FY 2007 FISMA independent 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, 14 of the 28 operational NRC information systems and 8 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation.

In FY 2009, the agency completed certification and accreditation of 12 agency systems and 1 contractor system. As of the completion of fieldwork for FY 2009, all but one of the operational NRC information systems had a current certification and accreditation, and all three of the systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation. The only system that was not certified and accredited is an aging mainframe system that is in the process of being replaced. Due to system development issues, the certification and accreditation of the replacement system is now scheduled for

[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.

[6] One agency system is currently not certified and accredited.

completion by the end of this calendar year. The operational legacy system did undergo annual security control testing in FY 2009.

3.3 Security Controls Testing (Question 2b)

OMB Requirement	OIG Response
2.b. Number of systems reviewed for which security controls have been tested and reviewed in the past year by FIPS 199 system impact level.	*See Table 3-3 below.*

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	8	1	9	2
Moderate	14	1	15	2
Low	0	1	1	0
Not Categorized	0	0	0	0
Total	22	3	25	4

Annual Security Control Testing – Background

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.

Security assessments are conducted to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to: (1) security certifications conducted as part of an information system accreditation or reaccreditation process, (2) continuous monitoring activities, or (3) testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. OMB does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must annually assess a subset of the security controls based on: (1) the FIPS 199 security categorization of the information system, (2) the specific security controls selected and employed by the organization to protect the information system, and (3) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system. It is expected that the organization will assess all of the security controls in the information system during the 3-year accreditation cycle. The organization can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement.

The FY 2009 FISMA guidance stated that agencies are required to use FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, for the specification of security controls and NIST SP 800-37 and SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, for the assessment of security control effectiveness.

The agency CIO issued a memorandum in January 2009 requiring system owners to complete annual contingency plan testing and annual security controls testing of all major applications and general support systems. System owners were required to prepare a schedule of planned contingency plan testing and annual security controls testing, with a completion date that does not exceed one year from the last time such testing was performed. Systems that were authorized to operate within the past fiscal year have already had their security controls tested and, therefore, do not require additional annual security control testing. The CSO identified a set of 48 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, with additional controls selected from the Access Control, Configuration Management, Contingency Planning, Incident Response, System Maintenance, and System and Services Acquisition control families. System owners were also required to select a subset of controls from the system's security plan that have not been assessed since the authority to operate was granted to the system or since the last annual security control testing was performed.

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

Twelve of the agency's 22 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 10 agency systems and 2 contractor systems required annual security control testing. As of the completion of fieldwork for FY 2009, annual security control testing was completed for the 10 agency systems and the 1 contractor system that required annual security control testing. In addition, while not required, the agency performed annual security control testing on two of the agency's operational systems that were authorized to operate in the past fiscal year.

3.4 Contingency Plan Testing (Question 2c)

OMB Requirement	OIG Response
2.c. Number of systems reviewed for which contingency plans have been tested in accordance with policy by FIPS 199 system impact level.	*See Table 3-4 below.*

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	8	1	9	2
Moderate	14	1	15	2
Low	0	1	1	0
Not Categorized	0	0	0	0
Total	22	3	25	4

Contingency Plan Testing – Background

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. Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, states that the NRC shall comply with the NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, IT risk assessments, and IT contingency plans) and other applicable NIST automated information security guidance for IT security processes, procedures, and testing. MD 12.5 also states that IT contingency plans for major applications and general support systems shall be tested each year. A live test provides the best indication of the adequacy of a contingency plan test. If a live test cannot be conducted due to operational constraints, a simulated test may be conducted in lieu of the live test. NRC Information Systems Security (ISS) and Office of Information Services (OIS) procedures also require annual contingency plan testing for all major applications and general support systems, including generating a contingency plan test report.

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

The agency CIO issued a memorandum in January 2009 requiring system owners to complete annual contingency plan testing and annual security controls testing of all major applications and general support systems. System owners were required to 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.

As of the completion of fieldwork for FY 2009, contingency plan testing[7] was completed for all 22 operational NRC information systems and for all 3 contractor systems. In addition, all 22 operational NRC information systems and all 3 contractor systems have current contingency plans.

3.5 Evaluation of Agency Oversight of Contractor Systems (Question 3a)

OMB Requirement	OIG Response
3.a. Does the Agency have policies for oversight of contractors?	*Yes*
3.a(1). Is the policy implemented?	*Yes*

Oversight of Contractor Systems – Background

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.[8]

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 re-accreditation 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.

[7] Any testing performed between September 1, 2008, and the completion of fieldwork would be considered as FY 2009 test results.

[8] 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.

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

Agency Oversight of Contractor Systems Meets FISMA Requirements

As of the completion of fieldwork for FY 2009, all three contractor systems for which NRC has direct oversight had a current certification and accreditation. One was authorized to operate in FY 2009 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.

3.6 Evaluation of Quality of Agency System Inventory (Questions 3b-3g)

OMB Requirement	OIG Response
3.b. Does the Agency have a materially correct inventory of major information systems (including national security systems) operated by or under the control of such Agency?	*Yes*
3.c. Does the Agency maintain an inventory of interfaces between the Agency systems and all other systems, such as those not operated by or under the control of the Agency?	*Yes*
3.d. Does the Agency require agreements for interfaces between systems it owns or operates and other systems not operated by or under the control of the Agency?	*Yes*
3.e. The Agency inventory is maintained and updated at least annually.	*Yes*
3.f. The IG generally agrees with the CIO on the number of Agency-owned systems.	*Yes*
3.g. The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the Agency or other organization on behalf of the Agency.	*Yes*

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.

MD and Handbook 12.5 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 CIO to establish procedures for interconnection of any IT device or system with the NRC IT infrastructure systems. It also specifies 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).

The agency's certification and accreditation process includes tasks, guidelines, and procedures for completing interconnecting security agreements. Two of the work breakdown elements are to establish agreements for needed interfaces and define interface specifications. Interconnection security agreements (ISA) and MOUs are required artifacts for inclusion in a certification and accreditation package (if applicable). The agency has developed procedures for creating ISAs and MOUs and has developed standard templates for these documents.

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 the new system.

FINDING A – The NRC Inventory Interface Information Is Still Inconsistent (Repeat Finding)

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's 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.

Carson Associates reviewed security plans, risk assessments, and other IT security documentation for the majority (19 of 25) of NRC and contractor 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 IT security documentation. 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 19 of 25 systems was inconsistent with information found in IT security documentation, as well as with interface information within NSICD. While there is more interface information in NSICD than was found during the FY 2008 independent evaluation, the information is still incomplete and inconsistent.

The guide that the agency developed for the CSO's administrative staff includes guidance on entering interface information into NSICD. However, it suggests obtaining this information from either the system's security categorization or risk assessment. These documents are not updated on a periodic basis, so the interface information found in these documents may not be current. Carson Associates also found that some of the security plans, which are required to be updated at least annually, did not include interface details, but referred the reader to other documents, which in some cases were not as current as the security plans. As a result, the interface information obtained from the security categorizations, risk assessments, and some security plans did not reflect the actual interfaces for the system.

On October 9, 2009, the agency reported the recommendations 1 and 2 from the FY 2008 FISMA independent evaluation as closed. Recommendation 1 should remain open until the agency corrects the inconsistencies that still exist in the inventory information in NSICD. Recommendation 2 should also remain open 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 IG suggests that the agency add additional guidance to the procedures on where to find current interface information, as well as how to ensure interface information remains consistent within NSICD.

RECOMMENDATION

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

1. Develop and implement procedures to ensure interface information is kept up-to-date.

3.7 Evaluation of Agency POA&M Process (Question 4)

OMB Requirement	OIG Response
4.a. Has the Agency developed and documented an adequate policy that establishes a POA&M process for reporting IT security deficiencies and tracking the status of remediation efforts?	*Yes*
4.a(1). Has the Agency fully implemented the policy?	*No*
4.b. Is the Agency currently managing and operating a POA&M process?	*Yes*
4.c. Is the Agency's POA&M process an Agency-wide process, incorporating all known IT security weaknesses, including IG/external audit findings 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?	*No*
4.d. Does the POA&M process prioritize IT security weaknesses to help ensure significant IT security weaknesses are corrected in a timely manner and receive appropriate resources?	*No*

OMB Requirement	OIG Response
4.e. When an IT security weakness is identified, do program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)?	*Yes*
4.f. For Systems Reviewed:	
4.f(1). Are deficiencies tracked and remediated in a timely manner?	*No*
4.f(2). Are the remediation plans effective for correcting the security weaknesses?	*Yes*
4.f(3). Are the estimated dates for remediation reasonable and adhered to?	*No*
4.g. Do program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly)?	*Yes*
4.h. Does the Agency CIO centrally track, maintain, and independently review/validate POA&M activities on at least a quarterly basis?	*Yes*

Agency POA&M Process – Background

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 shall 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.

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®[9] as change requests using the project management methodology process for change management. All certification and accreditation corrective actions arising

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

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 project management methodology process for change requests.

The agency has 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 also adds any new weaknesses identified from various sources including OIS recommendations and system certification artifacts. The agency provides instructions on providing the quarterly updates to the POA&M and specifies that data in only four fields on the POA&M should be changed: resources, brief description of work/services required, changes to milestones, and status.

The FY 2007 and FY 2008 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, and (2) the agency is not always following OMB and internal NRC POA&M guidance. Carson Associates also found that the agency is 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. Subsequent to the FY 2007 FISMA independent evaluation, the agency began analyzing a variety of tools to automate the POA&M process. 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 processes. However, the agency identified some problems with the tool, and after six months of research and evaluation the CSO picked Xacta, which was recently purchased, as the agency's tool for automating the POA&Ms.

The agency has also developed draft POA&M procedures to ensure quality assurance is emphasized. The draft procedures include 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 has 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 will take place quarterly targeting approximately 25 percent of the overall number of POA&Ms. Implementation of this process was scheduled for the third quarter of FY 2009, and the CSO plans to start meeting with the system owners in the first quarter of FY 2010.

The agency's new POA&M procedures also require corrective actions to be ranked based upon on the most critical security weaknesses and their impact on the agency's mission. This ranking should be reflected in the POA&M by listing identified weaknesses in priority order, irrespective of the weakness ID (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&M 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 B – The Quality of the Agency's POA&Ms Still Needs Improvement (Repeat Finding)

As in previous independent evaluations, Carson Associates found that the quality of the agency's POA&Ms still needs improvement. In assessing the agency's POA&M process, Carson Associates found that (1) the POA&M does not always include known IT security weaknesses, (2) deficiencies are not always remediated in a timely manner, and (3) estimated dates for remediation are not always adhered to.

In addition, Carson Associates found that the following problems identified with the POA&Ms in FY 2007 and FY 2008 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 owner.

The POA&M Does Not Always Include Known IT Security Weaknesses

The POA&M process is an agencywide process, but does not always include known IT security weaknesses from IG audits. The new agency POA&M procedures require new weaknesses to be added to the POA&M within 10 days of discovery. Carson Associates identified five OIG reports issued since May 2008 that identified IT security weaknesses. However, those weaknesses were not added to the POA&M until more than 6 months after the reports were issued. For example, the weaknesses from the FY 2008 FISMA independent evaluation were not added to the POA&M until the 4th Quarter FY 2009. In addition, the weaknesses for each report were added as one item on the POA&M for each report, instead of separate POA&M items for each weakness. Carson Associates also determined that none of the recommendations from the FY 2009 contingency plan testing, and not all of the weaknesses identified during the FY 2009 annual security control testing have been added to the POA&M.

Deficiencies Are Not Always Remediated in a Timely Manner

Carson Associates analyzed the POA&Ms for the four systems selected for evaluation in FY 2009 in order to characterize the timeliness of weakness remediation. Three of the four systems had at least one weakness that was closed more than 9 months after the scheduled completion date. One system had more than 25 percent of its closed weaknesses overdue by more than 9 months and 3 weaknesses that were closed over a year after their scheduled completion dates.

Estimated Dates for Remediation Are Not Always Adhered To

Carson Associates analyzed the POA&Ms for the four systems selected for evaluation in FY 2009 in order to determine if estimated remediation dates are adhered to. Three of the four systems have more than half of their open weaknesses more than 5 months overdue. One system has more than half of its open weaknesses overdue by more than 9 months.

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.
- Not counting weaknesses as closed when they have been closed by the OIG prior to the cutoff date for POA&M reporting.
- Reporting weaknesses as on track when they are actually delayed.
- Reporting weaknesses as delayed when they are still on track.

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

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

- Weaknesses with completion dates over a year old are not always removed from the POA&Ms. OMB guidance[10] 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&M.
- 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 POA&M items added to the 1st Quarter FY 2009 POA&M and the 4th Quarter FY 2009 POA&M did not have scheduled completion dates.
- Multiple weaknesses added under one POA&M item. Carson Associates identified five OIG reports issued since May 2008 that identified IT security weaknesses. The weaknesses for each report were added as one item on the POA&M for each report, instead of separate POA&M items for each weakness.

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

- 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 FISMA independent evaluation, 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 2009 annual security control testing, we found many instances where weaknesses that had been previously closed were still found to be present. In some instances, the weaknesses were added back to the POA&M with the FY 2009 annual security control testing results.

NRC Progress in Correcting Weaknesses Reported on Its POA&Ms Is Not Improving

The agency progress in correcting weaknesses reported on its POA&Ms is not improving. In FY 2007 the agency corrected 35 percent of its program level weaknesses and just over 23 percent of its system level weaknesses. In FY 2008 (quarters 1, 2, and 3), the agency corrected 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. However, in FY 2009 (FY 2008 4th quarter, and FY 2009 all quarters), the agency corrected 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.

RECOMMENDATION

The issue with the quality of the agency's POA&Ms is a repeat finding from the FY 2007 and FY 2008 FISMA independent evaluations. The recommendation from the FY 2007 FISMA independent evaluation is still open, as the agency has not completed all of their planned remediation activities. Therefore the OIG is not issuing a new recommendation for addressing this weakness.

3.8 IG Assessment of the Certification and Accreditation Process (Question 5)

OMB Requirement	OIG Response
5.a. Has the Agency developed and documented an adequate policy for establishing a certification and accreditation process that follows the NIST framework?	*Yes*
5.b. Is the Agency currently managing and operating a certification and accreditation process in compliance with its policies?	*Yes*
5.c. For Systems reviewed, does the certification and accreditation process adequately provide:	
5.c(1). Appropriate risk categories	*Yes*
5.c(2). Adequate risk assessments	*Yes*
5.c(3). Selection of appropriate controls	*Yes*

OMB Requirement	OIG Response
5.c(4). Adequate testing of controls	*Yes*
5.c(5). Regular monitoring of system risks and the adequacy of controls	*Yes*
5.d. For systems reviewed, is the Authorizing Official presented with complete and reliable certification and accreditation information to facilitate an informed system Authorization to Operate decision based on risks and controls implemented?	*Yes*

Certification and Accreditation – Background

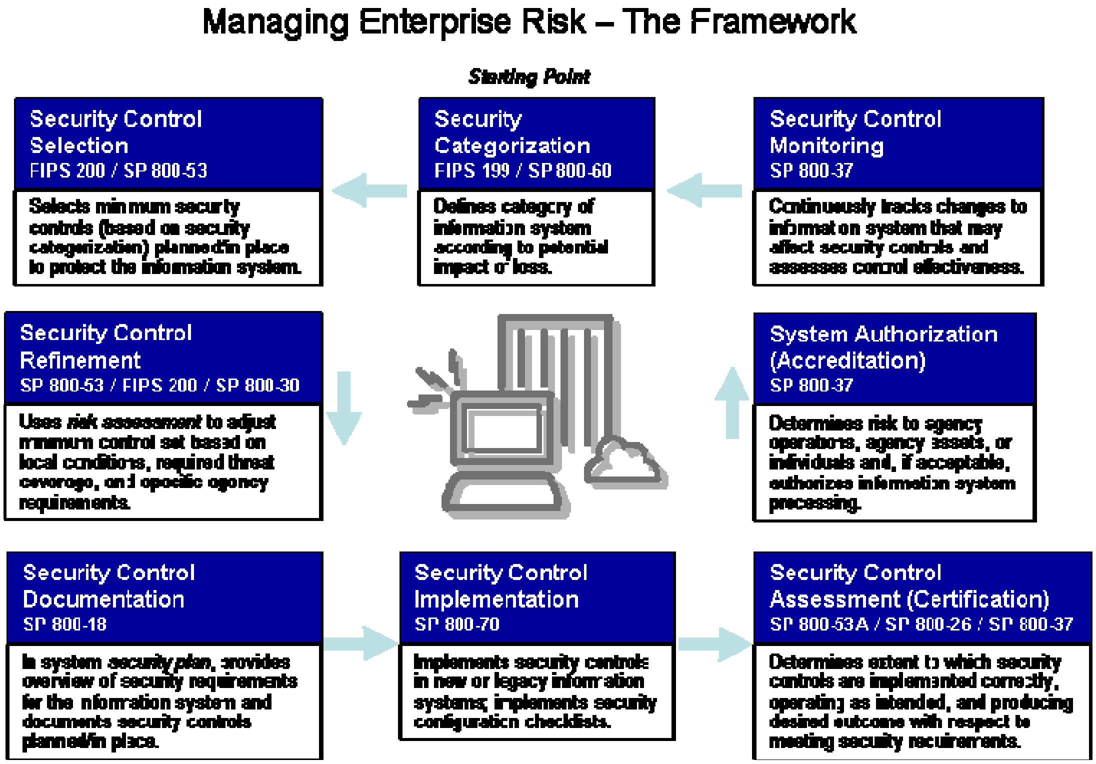
The security certification and accreditation of information systems is integral to an agency's information security program and is an important activity that supports the risk management process required by FISMA. Information systems under development must be certified and accredited prior to becoming operational. Operational information systems must be recertified and re-accredited every 3 years in accordance with Federal policy[11] and whenever there is a significant change[12] to the information system or its operational environment.

The following diagram[13] illustrates the key activities, including certification and accreditation, in managing enterprise-level risk, i.e., risk resulting from the operation of an information system. As illustrated in the diagram, NIST has developed several standards and guidelines to support the management of enterprise risk. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for certification and accreditation.

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

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

[13] 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).



Managing Enterprise Risk – The Framework

Starting Point

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

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

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

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

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

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

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

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

Security *certification* is a comprehensive assessment of the management, operational, and technical security controls[14] 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[15] 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.

[14] 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.

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

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

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

The NRC Certification and Accreditation Process Follows the NIST Framework

In order to evaluate the agency's certification and accreditation process, Carson Associates reviewed the certification and accreditation process and procedures located on the agency's project management methodology Web site, and reviewed accreditation decision memoranda issued by the agency's authorizing official. NRC's certification and accreditation process is documented on their Project Management Methodology (PMM) Web site and is part of the agency's 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.

NRC Is Managing and Operating a Certification and Accreditation Process In Compliance With Its Policies

To determine if the agency is managing and operating a certification and accreditation process in compliance with its policies, we reviewed the certification and accreditation documents for the four systems selected for evaluation during the FY 2009 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 process adequately provides:

- Appropriate risk categories.
- Adequate risk assessments.
- Selection of appropriate controls.
- Adequate testing of controls.
- Regular monitoring of system risk and the adequacy of controls.

Carson Associates also determined that for the four systems selected for evaluation, the Authorizing Official was presented with complete and reliable certification and accreditation information to facilitate an informed Authorization to Operate decision based on risks and controls implemented.

3.9 IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process (Question 6)

OMB Requirement	OIG Response
6.a. Has the Agency developed and documented adequate policies that comply with OMB guidance in M-07-16, M-06-15, and M-06-16 for safeguarding privacy-related information?	*Yes*
6.b. Is the Agency currently managing and operating a privacy program with appropriate controls in compliance with its policies?	*Yes*
6.c. Has the Agency developed and documented an adequate policy for PIAs?	*Yes*

OMB Requirement	OIG Response
6.d. Has the Agency fully implemented the policy and is the Agency currently managing and operating a process for performing adequate PIAs?	*Yes*

Policies That Comply With OMB Guidance in M-07-16, M-06-15, and M-06-16 Exist

On March 20, 2009, the OIS Director reported on the agency's progress in reducing the risks related to the breach of PII to the Commission. For example, since 2006, nine yellow announcements have been issued implementing the OMB guidance. In addition, the staff has reviewed all agency forms, removed the unnecessary collections of PII, and revised the forms as appropriate. The staff has also developed a contract clause for protecting PII that may be provided, collected, used, possessed, or processed in the course of performing work under an NRC contract. The memorandum included as an attachment a comprehensive progress report on all of the actions taken by the staff and the actions still to be completed. The following are some of the actions taken by the agency to protect PII.

The following agency policies, procedures, and guidance have been developed and documented in compliance with OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*:

- Yellow Announcement YA-08-0093, Information Technology Implementation Policy – Updated Computer Security Incident Response and PII Incident Response, July 3, 2008: Announced revised computer security incident policy to include direction for responding to PII incidents.
- *Computer Security Incident Response Policy*, July 3, 2008.
- Yellow Announcement YA-07-0106, Safeguarding Against and Responding to the Breach of PII, September 19, 2007: Distributed OMB M-07-16 to all NRC employees, and announced publication of the *NRC PII Breach Notification Policy* and the *NRC Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers (SSNs)*.
- *PII Breach Notification Policy*, September 19, 2007, updated February 9, 2009, to include credit monitoring services under certain circumstances to individuals whose PII has been unintentionally breached by NRC.
- Yellow Announcement YA-07-0096, Guidance for Periodic Review of Agency Network Drives for the Presence of PII, September 6, 2007: The NRC will review all agency-shared drives for the purpose of identifying and eliminating PII at least annually. The FY 2008 review was completed September 19, 2008.
- *Plan to Eliminate the Unnecessary Collection and Use of SSNs*, September 19, 2007. A progress update was issued September 19, 2008.
- Electronic PII is discussed in the U.S. NRC *Agency-wide Rules of Behavior for Authorized Computer Use*, May 19, 2009. The rules of behavior are provided to NRC computer users as part of the annual computer security awareness 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. Violation

of these rules will be reported to the user's management and to the CSO. Non-compliance may subject the user to disciplinary action, as well as penalties and sanctions, including verbal or written warning, removal of system access privileges, reassignment to other duties, criminal or civil prosecution, and/or removal from Federal service, depending on the severity of the violation.

- The agency is currently developing annual PII responsibilities awareness and acknowledgement.

The following agency policies, procedures, and guidance have been developed and documented in compliance with OMB M-06-16, *Protection of Sensitive Agency Information*:

- Yellow Announcement YA-09-0035, Information Technology Security Policy – Laptop Security Policy, April 2, 2009: Announced new policy for laptop security, including requirement that laptops use full disk encryption.
- *Laptop Security Policy*, April 2, 2009.
- Yellow Announcement YA-08-157, Information Technology Security Policy – Encryption of Data at Rest, December 19, 2008: Announced new encryption of data at rest policy and NUREG/BR-168, Revision 4.
- *Computer Security Policy for Encryption of Data at Rest When Outside of Agency Facilities*, Effective December 31, 2008
- NUREG/BR-0168, Revision 4, *Guide for IT Security, Policy for Processing Unclassified Safeguards Information on NRC Computers*, Effective December 31, 2008.
- Yellow Announcement YA-06-0069, Protection of PII, September 19, 2009 (regarding requirement #2 from OMB M-06-16): NRC remote broadband access through Citrix implements two-factor authentication by requiring two separate object authentications to obtain access to the NRC remote access services: (1) a digital certificate and (2) a user name and password. The user name and password are not stored on the workstation and are independent of the digital certificate authentication. However, it does not meet the criterion for "a device separate from the computer gaining access." Because the risk associated with the lack of a separate device is low, the Executive Director for Operations endorsed access to PII through Citrix broadband at this time. The staff will be further evaluating the use of a separate device as part of our long-term actions. In the interim, the staff is prohibited from accessing systems containing PII through a dial-up modem unless they use an NRC laptop that is configured in accordance with security requirements approved by OIS. This prohibition does not apply to employees remotely accessing the Human Resources Management System or Employee Express to update their own personal information. Implementation of true two-factor authentication is to be implemented in FY 2011.
- Yellow Announcement YA-08-092, Information Technology Implementation Policy – Computer Security Information Protection Policy, June 26, 2008: Announced revised Computer Security Information Protection Policy to address the time-out requirement in M-06-16.
- Computer Security Information Protection Policy, June 26, 2008: Remote access to any system that processes non-public NRC information shall be constrained by a "time-out"

function that requires re-authentication after 30 minutes of inactivity. Mobile device access to any non-public NRC information shall be constrained by a "time-out" function that requires re-authentication after 30 minutes of inactivity.

- On September 16, 2008, the agency issued a memorandum regarding a new policy for logging and erasure of all computer-readable data extracts from databases holding sensitive information. The purpose of the memorandum is to expand upon previously issued policies and yellow announcements regarding the protection of sensitive information. The purpose of this policy is to ensure that Office Directors and Regional Administrators are aware of their responsibility to know where their sensitive information resides, when that information leaves their office's control, and that the information is appropriately protected.

  On February 12, 2009, the NRC EDO withdrew the above-mentioned policy for logging and erasure of all computer-readable extracts from databases holding sensitive information. As most agencies are struggling with finding a way to implement the database extract logging requirement, OMB is reexamining the requirement and will be providing new guidance. Once the new guidance is received, the agency will issue an appropriate policy. The requirement to log extracts of PII specified in YA-2006-069 remains in effect.

The following agency policies, procedures, and guidance have been developed and documented in compliance with OMB M-06-15, *Safeguarding Personally Identifiable Information*:

- The agency sends out periodic reminders, typically via yellow announcement, to employees about their responsibilities for safeguarding PII, the rules for acquiring and using such information, as well as penalties for violating these rules. Announcements are sent at least once a year and can also be found on the agency's Privacy Act Program Web page.
- The agency conducts reviews of agency policies and processes and has included the results of those reviews with their annual FISMA submissions, as directed by OMB, since the FY 2006 FISMA submission.
- On January 22, 2009, via yellow announcement, the agency announced the republication of the agency's Privacy Act systems of records notices. The notices were published in their entirety in the Federal Register on January 6, 2009. The yellow announcement reminded employees of their responsibility to familiarize themselves with current guidance and procedures addressing privacy at the NRC and included links to NRC internal Web pages related to privacy at the NRC.

NRC Is Managing and Operating a Privacy Program In Compliance With Its Policies

The agency is managing and operating a privacy program, which is described in MD and Handbook 3.2, *Privacy Act*, dated June 27, 2007. The agency also maintains a Privacy Act Program Web site, which includes guidance on various topics related to the Privacy Act. The agency also maintains a separate Web page dedicated to the protection of PII. This Web page describes the agency's activities related to the protection of PII and contains information such as (1) frequently asked questions; (2) how to report inadvertent releases of PII; (3) links to OMB, Office of Personnel Management, and NRC PII policy; (4) information on the agency's PII task force (e.g., background and charter, membership, and meeting minutes); and (5) information on automated tools available to assist in searching for files that contain PII.

A Policy for PIAs Has Been Developed and Documented

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

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

MD and Handbook 3.2 requires office directors and regional administrators to ensure that PIAs are prepared and submitted to OIS before developing or procuring IT that collects, maintains, or disseminates personal information about individuals or when initiating a new electronic collection of personal information in identifiable form[16] from 10 or more persons. In accordance with the agency's project management methodology, a PIA is required for all investments at the inception phase of the development life cycle. PIAs are also part of the agency's certification and accreditation process. ISS-01-001, Revision 0, *PIA Procedures*, dated August 30, 2006, requires a PIA (or update of an existing PIA) for each legacy system requiring recertification and re-accreditation.

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

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

Does the agency have a written policy or process for evaluating changes in business process or technology that the PIA indicates as necessary?

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

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

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

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

Does the agency have a written policy or process for making PIAs available to the public in the required circumstances and for making PIAs available in other than required circumstances?

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

NRC Has Fully Implemented Its PIA Policy and is Managing and Operating a Process for Performing PIAs

To determine if the agency has fully implemented the PIA policy and is currently managing and operating a process for performing adequate PIAs, we reviewed the PIAs for the four systems selected for evaluation during the FY 2009 independent evaluation. The PIAs were completed and reviewed in accordance with NRC policy. The Privacy Act does not apply to three of the systems and does apply to one of the systems.

3.10 Configuration Management (Question 7)

3.10.1 Security Configuration Policy and Common Security Configurations

OMB Requirement	OIG Response
7.a. Is there an Agency-wide security configuration policy?	*Yes*
7.b. For each OS/platform/system for which your Agency has a configuration policy, please indicate the status of implementation for that policy.	

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

The agency has also posted guidance on the NRC internal Web site requiring the use of hardening specifications for the different operating systems and software in use at the agency. Hardening specifications in use at the agency include benchmarks developed by the Center for Internet Security (CIS), the Defense Information Systems Agency (DISA) Gold Disk,[17] National Security Agency (NSA) security configuration guides, and custom hardening specifications developed by the agency. The agency requires the use of the most recent version of the specified hardening specifications.

NRC Security Configuration Policy

The agency's security configuration policy is described in the system screening guidelines for the NRC network, and on the CSO's Standards Web page. In addition, all systems are required to undergo vulnerability scanning and penetration testing as a part of security test and evaluation during the certification and accreditation process. The purpose of the vulnerability scanning and penetration is, in part, to determine whether the system's configuration is compliant with the established agency configuration standards.

The NRC has established a configuration policy for the following operating systems, platforms, and systems:

NRC-Developed

- Stealth MXP Thumb Drive Configuration Standard
- NRC General Laptop Configuration Guidance
- NRC Laptop Configuration Standards
- Linux Red Hat Hardening Guidelines
- VMWare Hardening Guidelines
- Microsoft Windows 2003 Servers

[17] 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.

- NRC Web 2.0 Implementation Standard
- NRC YouTube Standard

<u>Industry Standards (e.g., CIS Benchmarks, DISA standards, and/or NSA standards)</u>

- AIX
- HP-UX
- Mac OS X Systems
- Novell NetWare
- Solaris
- Microsoft Windows 2000 Servers
- Microsoft Windows 2008 Servers
- Microsoft Window XP Professional
- Microsoft Windows 2000 Professional
- Microsoft Windows 2003 Security Checklist
- Microsoft Windows 2008 Security Checklist
- Microsoft Exchange 2003 Security Technical Implementation Guide
- Cisco IOS Router (Level 1 and Level 2)
- Cisco PIX Firewall (Level 1 and Level 2)
- Apache Web Server (Level 1 and Level 2)
- Exchange Server 2003
- Oracle Database 8i (Level 1 and Level 2)
- Oracle Database 9i (Level 1 and Level 2)
- Oracle Database 10g (Level 1 and Level 2)
- SQL Server 2000 (Level 1 and Level 2)
- Internet Explorer
- Internet Information Services V 5.0
- Internet Information Services V 5.0
- Microsoft Office
- Netscape Navigator
- Microsoft .NET Framework
- Systems Management Servers 2003

NRC Security Configuration Policy Implementation Status

To determine the status of the implementation of agency configuration policies, Carson Associates reviewed various security documentation for the four systems selected for evaluation in FY 2009, including security plans, security test and evaluation reports, and vulnerability assessment reports. The agency performs a vulnerability assessment during security control testing, which includes vulnerability scans, penetration tests, and hardening checks using the following tools:

- Nessus – A general-purpose scanning tool that provides information on network-based vulnerabilities.
- 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.
- CORE Impact – A specialized penetration testing tool that provides automated testing of known exploits against detected platforms, protocols, and services.
- CIS Benchmarks – NRC-approved security hardening specifications for a variety of platforms and software, prepared by CIS (http://www.cisecurity.org/).
- NRC Linux Benchmark – An NRC-approved security hardening specification for the Linux systems that was developed from the Red Hat Linux Benchmark by CIS.

The following operating systems, platforms, and systems were identified for the four systems selected for evaluation in FY 2009.

- IBM AIX 5
- Cisco IOS
- Cisco PIX Firewall
- Red Hat Enterprise Linux 4
- Sun Solaris 10
- Microsoft SQL Server 2000
- Microsoft SQL Server 2005
- Microsoft Windows Server 2000
- Microsoft Windows Server 2003
- Microsoft Windows NT
- Microsoft Windows XP

While the agency has a configuration policy for additional operating systems, platforms, and systems, Carson Associates could only form an opinion on the status of the implementation of agency configuration policies for those operating systems, platforms, and systems found in the four systems selected for evaluation in FY 2009. Carson Associates determined that the implementation status of the relevant policies is mid-implementation.

3.10.2 Federal Desktop Core Configuration (FDCC)

OMB Requirement	OIG Response
7.c. Indicate the status of the implementation of Federal Desktop Core Configuration (FDCC) at your Agency:	
7.c(1). Agency has documented deviations from FDCC standard configuration.	*Yes*
7.c(2). New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology," is included in all contracts related to common security settings.	*No*

Carson Associates reviewed several agencywide announcements and determined that the agency has adopted and implemented FDCC standard configurations. Carson Associates reviewed the agency's reports to OMB and 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 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 OIS has 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 Safeguards Information (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 memo 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. 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 has deployed NIST-validated Security Content Automation Protocol (SCAP) scanning tools to scan a sample of network hosts. Standalone computers are scanned periodically as they are brought in for service. The SCAP tools are also used to verify that the agency is compliant with FDCC during the system certification and accreditation process. 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. This completion of the IAS will provide agencywide, real-time FDCC assessments. The system is currently scheduled for completion in FY 2010.

The agency also 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.

In the agency's September 5, 2008, FDCC status update to OMB, the agency reported the following:

• Total number of managed desktops and laptops (Windows XP SP2):	5,077
• Total number of XP desktops and laptops that are FDCC compliant:	0

The agency has adopted and implemented FDCC standard configurations and has documented the deviations. Of the 354 settings that were tested: 332 settings passed, 22 settings failed. The raw score is 93.8 percent. Of the 22 settings that failed, one setting does not apply to Internet Explorer version 6, and so is a false failure. Three settings reference a local support account that does not exist on the desktops/laptops in the NRC environment, thus resulting in failures. However, restrictions are set appropriately in the group policy. The remaining 18 settings that failed FDCC compliance have been documented. Taking these four settings into account, the NRC passes 332 settings out of 350 applicable settings. The adjusted score is 94.8 percent.

The Division of Contracts has updated their contracts writing system to include the revised policy in Federal Acquisition Regulation 39.101. However, the CSO and Office of Administration, Division of Contracts are still in the process of developing standard contract language and clauses that specify which IT security policies and requirements, including the use of common security configurations, should be included in IT acquisition contracts as required by Federal Acquisition Regulation 39.101. It should be noted that the agency does include some IT security-related sections and references in their IT acquisition contracts, including NRC IT security training, NRC Management Directives and Handbooks related to security, badge requirements for unescorted access to NRC facilities, and security requirements for IT access approval.

3.11 Incident Reporting (Question 8)

OMB Requirement	OIG Response
8.a. How often does the Agency comply with documented policies and procedures for identifying and reporting incidents internally?	*91% to 100%*
8.b. How often does the Agency comply with documented policies and procedures for timely reporting of incidents to US-CERT?	*91% to 100%*
8.c. How often does the Agency comply with documented policy and procedures for reporting to law enforcement?	*91% to 100%*

On May 2, 2008, the agency issued a revised policy on computer security incident response and 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 12.5. The revised policy contains time frames for responding to such incidents, based on the criticality of the affected resources and the incident; formally establishes a Computer Security Incident Response Team (CSIRT) to respond to such incidents; and outlines the CSIRT's security incident response process. The CSIRT will include staff from the following offices: CSO, OIS, Office of Administration, and Office of Nuclear Security and Incident Response.

In addition to forming CSIRT, the agency has 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.[18]

- Computer Security Incident Response Policy, May 14, 2008.
- Information Systems Security Incident Response Procedures, May 11, 2004 (Appendix B from MD 12.5).
- Draft CSIRT Responder Guide, February 25, 2009.
- Draft CSIRT Standard Operating Procedures, October 30, 2008.

The agency uses two tools for tracking incidents. An incident report form is used to capture the full details of each incident reported to or discovered by the incident response team. An incident response tracking sheet is used to capture summary information for each incident. This tracking sheet provides high-level metrics regarding all incidents. The team performs self-audits of the incident report forms to ensure there is a form for each entry on the tracking sheet and that each entry on the tracking sheet has a corresponding incident report form. This self-audit is performed at least quarterly.

CSIRT also conducts periodic incident response testing. The most recent test was in June 2009. The agency performed a table-top exercise of the CSIRT response to a Category 1 incident (unauthorized access). The test results were documented and included 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 included a checklist of actions that should have been taken during the exercise and documented lessons learned.

In order to determine how often the agency complies with documented policies and procedures related to incident reporting, Carson Associates met with NRC staff responsible for incident reporting and reviewed the incident response tracking form used by the agency.

[18] 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, who then decides whether or not external law enforcement should be involved.

3.12 Security Awareness Training (Question 9)

OMB Requirement	OIG Response
9.a. Has the Agency developed and documented an adequate policy for identifying all general users, contractors, and system owners/employees who have log-in privileges, and providing them with suitable IT security awareness training?	*Yes*
9.b. Report the following for your Agency:	
9.b(1). Total number of people with log-in privileges to Agency systems.	*4,840*
9.b(2). Number of people with log-in privileges to Agency systems that received information security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program."	*4,730 (98%)*
9.b(3). Total number of employees with significant information security responsibilities.	*403*
9.b(4). Number of employees with significant security responsibilities that received specialized training, as described in NIST SP 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model."	*130 (32%)*

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, which includes a discussion on appropriate use of information technology 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 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.

<u>Annual IT Security Awareness Training</u>

NRC meets the Office of Personnel Management requirement to expose employees to security awareness materials at least annually by (1) mandating all NRC staff take annual IT security awareness training and by documenting who takes the annual training; and (2) using posters, flyers, Web pages, and NRC announcements.

For FY 2009, 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 cut-off date of August 3, 2009, for completion of the course. The self-paced course consisted of two modules – a general computer security awareness training module using ISS Line of Business (LoB) approved courseware tailored to the general federal population, and an NRC-specific module tailored to address 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 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 2009 training. Office training coordinators were required to track completion of the computer security awareness course and report weekly completion percentages to the CSO's office. In an announcement dated August 4, 2009, the agency reported 4,726 users had completed the FY 2009 computer security awareness course – the equivalent of 97 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 IT security awareness training by office.

IT Security Awareness Training for Employees With Significant IT Security Responsibilities (Role-Based Training)

On April 3, 2008, the CISO issued a memorandum asking for support and action to ensure that all employees with significant IT security responsibilities are appropriately identified. The memorandum requires recipients of the memorandum to report back to the CISO by July 1, 2008, on the names of employees within their organization that have an IT security role as part of their official duties. A second data call was issued July 13, 2009, asking recipients of the memorandum to review and update the information provided in response to the April 2008 data call. The memorandum requires recipients to report back to the CSO by August 10, 2009.

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 his/her 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 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 ISSO course was updated in June 2009, and the system and network administrator course was updated in December 2008. In addition, the agency provided a Defense in Depth – Securing Windows Server 2003 course to approximately 20 employees in January 2008 and provided role-based training for system owners in August 2008. The CSO also provided system administrators and ISSOs with a Microsoft Framework Essentials 4.0 Managing Change/Configuration/Risk course. The CSO is working with a contractor to draft and present additional specific role-based courses that address the following roles: ISSO, System Administrator, IT Manager, System Owner, Executive, and Senior Manager.
- **ISS LoB Providers:** The CSO coordinated with the Department of Defense for the use of its ISS LoB approved courseware for agencywide 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.

3.13 Peer-to-Peer File (P2P) Sharing (Question 10)

OMB Requirement	OIG Response
10. Does the Agency explain policies regarding the use of peer-to-peer file sharing in IT security awareness training, ethics training, or any other Agency-wide training?	*Yes*

In 2007, the Executive Director for Operations in a memorandum to the Commission recommended prohibiting the installation of P2P software on NRC computers without explicit written approval of the NRC Designated Approving Authority. In February 2008, the agency issued a yellow announcement on P2P software that states:

> All employees, including staff and contractors, are prohibited from installing P2P software on agency computers without the explicit written approval of an agency Designated Approving Authority. In addition, employees are prohibited from processing Sensitive Unclassified Non-Safeguards Information (SUNSI) on home computers unless connected to and working within CITRIX, the NRC Broadband Remote Access System. Employees are prohibited from downloading or storing SUNSI to the hard drive of a home computer when connected to and working within CITRIX. Employees are also prohibited expressly from processing SUNSI

> on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media. Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX; or (2) an NRC-issued laptop with NRC-approved encryption software.

The CSO's IT Security Policies Web page specifically states that the installation of P2P software on NRC computers is prohibited unless explicitly approved by the NRC Designated Approving Authority in writing. The CSO's Web site also provides some P2P frequently asked questions. The FY 2009 online computer security awareness course discussed the use of P2P and file-sharing software.

[Page intentionally left blank]

4 Report Recommendation

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

1. Develop and implement procedures to ensure interface information is kept up-to-date.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on October 30, 2009, agency officials agreed with the report's findings and recommendation 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 2009. 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 2009 and September 2009. 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; Virgil Isola, CISSP; and Edwin Caron, CISA, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]