

EVALUATION REPORT

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2011

OIG-12-A-04 November 9, 2011



All publicly available OIG reports (including this report) are accessible through
NRC's Web site at:

<http://www.nrc.gov/reading-rm/doc-collections/insp-gen/>



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

**OFFICE OF THE
INSPECTOR GENERAL**

November 9, 2011

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S
IMPLEMENTATION OF THE FEDERAL INFORMATION
SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL
YEAR 2011 (OIG-12-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 (FISMA) for Fiscal Year 2011 (OIG-12-A-04)*.

The report presents the results of the subject evaluation. Agency comments provided during a November 3, 2011, exit conference have been incorporated, as appropriate, into this report.

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

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

Attachment: As stated



**Independent Evaluation of
NRC's Implementation of the
Federal Information Security Management Act
for Fiscal Year 2011**

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

November 09, 2011

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002.¹ FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program² 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 Office of the Inspector General (OIG) or by an independent external auditor. Office of Management and Budget (OMB) memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

Richard S. Carson & Associates, Inc. (Carson Associates), performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2011. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool.

This report reflects the status of the agency's information security program for FY 2011.

PURPOSE

The objective of this review was to perform an independent evaluation of the NRC's implementation of FISMA for FY 2011.

RESULTS IN BRIEF

Program Enhancements and Improvements

Over the past 9 years, NRC has continued to make improvements to its information system security program and continues to make progress in implementing the recommendations resulting from previous FISMA evaluations. The agency has accomplished the following since the FY 2010 FISMA independent evaluation:

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

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

- The agency continued to make significant progress in assessing and authorizing its systems.³ In FY 2011, the agency completed security assessment and authorization of two new agency systems, and completed security assessment and re-authorization of two existing agency systems, and one existing contractor system.⁴ As of the completion of fieldwork for FY 2011, all 22 operational NRC information systems and both systems used or operated by a contractor or other organization on behalf of the agency had a current authorization to operate.
- The agency completed or updated security plans for all of the agency's 22 operational systems and for both 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, including updating the contingency plans.
- The agency issued several new or updated Computer Security Office processes and standards including the NRC Risk Management Framework (RMF) and Authorization Process (new), a series of standards defining the values NRC has assigned for the 17 families of security controls (new), the NRC System Back-up Standard (new), and the NRC Plan of Action and Milestones (POA&M) Process (updated).

Program Weaknesses

While the agency has continued to make improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified three information system security program weaknesses.

- There is a repeat finding from several previous independent evaluations: the agency's POA&M program still needs improvement.
- The agency has not developed an organizationwide risk management strategy.
- Configuration management procedures are not consistently implemented.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA. A consolidated list of recommendations appears on page 37 of this report.

³ With the issuance of NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, the terms certification and accreditation are no longer being used. The new terminology is security assessment and authorization.

⁴ The Licensing Support Network was decommissioned subsequent to re-authorization. This system is no longer included in the agency's inventory of contractor systems.

AGENCY COMMENTS

At an exit conference on November 3, 2011, agency officials agreed with the report's findings and recommendations and provided a few editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

ASCT	Annual Security Control Testing
ATU	Authorization to Utilize
BIA	Business Impact Assessment
Carson Associates	Richard S. Carson and Associates, Inc.
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CPIC	Capital Planning and Investment Control
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
DAA	Designated Approving Authority
DEDO	Deputy Executive Director for Operations
DISA	Defense Information Systems Agency
EDO	Executive Director for Operations
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GAO	Government Accountability Office
IM	Information Management
ISSO	Information Systems Security Officer
IT	Information Technology
ITBC	IT/IM Business Council
ITSAC	IT/IM Senior Advisory Council
ITSPG	IT/IM Strategic Planning Group
MD	Management Directive
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSICD	NRC System Information Control Database
OIG	Office of the Inspector General
OIS	Office of Information Services
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PMM	Project Management Methodology

POA&M	Plan of Action and Milestones
RMF	Risk Management Framework
SCAP	Security Content Automation Protocol
SIGI	Safeguards Information
SP	Special Publication
ST&E	Security Test and Evaluation
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline

TABLE OF CONTENTS

Executive Summary	i
Abbreviations and Acronyms	v
1 Background.....	1
2 Objective.....	1
3 Findings.....	1
3.1 FISMA Systems Inventory	2
The NRC System Inventory Meets FISMA Requirements.....	3
3.2 Risk Management (Question 1).....	4
The NRC Risk Management Program Needs Improvement.....	4
3.2.1 Risk Management Program	5
NRC Has Not Developed an Organizationwide Risk Management Strategy	7
3.2.2 Risk Management Framework	7
All Major Applications and General Support Systems Have Been Categorized in Accordance with NRC Policy	9
Security Plans Have Been Developed or Updated in Accordance with NRC Policy	9
All Agency Systems Have a Current Authorization To Operate	9
3.3 Configuration Management (Question 2).....	10
The NRC Security Configuration Management Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines.....	10
Standard Baseline Configurations Are Not Implemented on Some NRC Systems	12
Software Compliance Assessment Procedures Are Not Consistently Implemented	13
Vulnerability Remediation and Patch Management Procedures Are Not Consistently Implemented.....	14
3.4 Incident Response and Reporting (Question 3)	16
The NRC Incident Response and Reporting Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines.....	16
3.5 Security Training (Question 4).....	19
The NRC Security Training Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines	19
3.6 POA&M (Question 5).....	21
The NRC POA&M Program Needs Improvement	22
POA&Ms Do Not Include All Known Security Weaknesses	24
Initial Target Remediation Dates Are Still Often Missed.....	24
POA&Ms Are Not Updated in a Timely Manner	25
3.7 Remote Access (Question 6).....	25
The NRC Remote Access Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines	25
3.8 Identity and Access Management Program (Question 7)	26

The NRC Identity and Access Management Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines	27
3.9 Continuous Monitoring Management (Question 8)	28
The NRC Continuous Monitoring Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines	29
NRC Has Completed Annual Security Control Testing for All Agency and Contractor Systems	30
3.10 Contingency Planning (Question 9).....	30
The NRC Business Continuity/Disaster Recovery Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines.....	30
Annual Contingency Plan Testing Was Completed for All Agency Systems and All Contractor Systems	31
3.11 Contractor Systems (Question 10)	31
The NRC Contractor Oversight Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines	32
Agency Oversight of Contractor Systems Meets FISMA Requirements.....	33
3.12 Security Capital Planning (Question 11)	33
The NRC CPIC Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines	33
4 Consolidated List of Recommendations	37
5 Agency Comments	39
Appendix. OBJECTIVE, SCOPE, AND METHODOLOGY.....	41

List of Tables

Table 3-1. Total Number of Agency and Contractor Systems and Number Reviewed by FIPS 199 System Impact Level	4
---	----------

List of Figures

Figure 1: Tiered Risk Management Approach (source: NIST SP 800-37, Revision 1)....	5
Figure 2: Risk Management Framework (source: NIST SP 800-37, Revision 1).....	8

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. 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 Office of the Inspector General (OIG) or by an independent external auditor. Office of Management and Budget (OMB) memorandum M-11-33, *FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated September 14, 2011, requires OIG to report their responses to OMB's annual FISMA reporting questions for OIGs via an automated collection tool.

Richard S. Carson & Associates, Inc. (Carson Associates), performed an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2011. This report presents the results of that independent evaluation. Carson Associates also submitted responses to OMB's annual FISMA reporting questions for OIGs via OMB's automated collection tool.

This report reflects the status of the agency's information security program for FY 2011.

2 Objective

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2011. The appendix contains a description of the evaluation objective, scope, and methodology.

3 Findings

Over the past 9 years, NRC has continued to make improvements to its information system security program and continues to make progress in implementing the recommendations resulting from previous FISMA evaluations. The agency has accomplished the following since the FY 2010 FISMA independent evaluation:

- The agency continued to make significant progress in assessing and authorizing its systems. In FY 2011, the agency completed security assessment and authorization of two new agency systems, and completed security assessment and re-authorization of two existing agency systems, and one existing contractor system. As of the completion of fieldwork for FY 2011, all 22 operational NRC information systems and both systems used or operated by a contractor or other organization on behalf of the agency had a current authorization to operate.
- The agency completed or updated security plans for all of the agency's 22 operational systems and for both 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, including updating the contingency plans.
- The agency issued several new or updated Computer Security Office processes and standards including the NRC Risk Management Framework (RMF) and Authorization Process (new), a series of standards defining the values NRC has assigned for the 17 families of security controls (new), the NRC System Back-up Standard (new), and the NRC Plan of Action and Milestones (POA&M) Process (updated).

While the agency has continued to make improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified three information system security program weaknesses.

- There is a repeat finding from several previous independent evaluations: the agency's POA&M program still needs improvement.
- The agency has not developed an organizationwide risk management strategy.
- Configuration management procedures are not consistently implemented.

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

3.1 FISMA Systems Inventory

FISMA requires agencies to develop and maintain an inventory of major information systems (including major national security 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. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, control PM-5, Information System Inventory, requires organizations to develop and maintain an inventory of its information systems.

Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, also define requirements for the agency's inventory of automated information systems. The agency's inventory must identify all interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency.

The NRC System Inventory Meets FISMA Requirements

Previous FISMA independent evaluations found that the agency's official inventory repository, NRC System Information Control Database (NSICD), did not include complete interface information and that the majority of the interface in NSICD was inconsistent with information included in information technology (IT) security documentation, as well as with interface information within NSICD. While interface information can be found in other locations and documentation, FISMA requires that 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." In response to recommendations from previous independent evaluations, the agency updated NSICD to include interface information for all systems in the NRC inventory. The agency also updated a guide for the Computer Security Office (CSO) administrative staff for entering data into security records within NSICD to ensure interface information is consistent with interface information in security plans and risk assessments and to ensure interface information is kept up-to-date. The agency's continuous monitoring program also includes requirements for reviewing system interfaces.

Carson Associates reviewed security plans for 22 systems to identify the interfaces for those systems. Carson Associates then reviewed the records for those systems in NSICD to determine if the agency's inventory included the interfaces identified in the security plans. Carson Associates also analyzed the interface information in NSICD for consistency within the inventory.

As of completion of fieldwork, NRC had 22 operational systems that fall under FISMA reporting requirements.⁵ Of the 22, 10 are general support systems,⁶ and 12 are major applications.⁷ NRC had two systems operated by a contractor or other organization on behalf of the agency (two general support systems). Of the two, one is operated by a federally funded research and development center, and one is operated by a private contractor. As required by FISMA, Carson Associates selected a subset of NRC systems and contractor systems for evaluation during the FY 2011 FISMA independent evaluation. Subsequent to the start of field work, the contractor system selected for evaluation was decommissioned by the agency. Therefore, no contractor systems were included in the FY 2011 evaluation.

⁵ NRC also has a number of major applications and general support systems currently in development. For FISMA reporting purposes, only operational systems are considered.

⁶ 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.

⁷ A major application is a computerized information system or application that requires special attention to security because of the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.

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

FIPS 199 System Impact Level	Agency Systems		Contractor Systems		Total Number of Systems (Agency and Contractor Systems)	
	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
High	9	1	1	0	10	1
Moderate	13	2	1	0	14	2
Low	0	0	0	0	0	0
Not Categorized	0	0	0	0	0	0
Total	22	3	2	0	24	3

NOTE: The agency is in the process of reorganizing some of its infrastructure systems by consolidating one existing system into another existing system and is also separating a portion of that same existing system into a new, separate system. The existing system is in the process of being re-authorized to operate to reflect the changes and the new system is also in the process of being authorized to operate as a separate system. As a result of this reorganization, the number of reportable systems at the agency will remain at 24.

3.2 Risk Management (Question 1)

FISMA requires agencies to perform periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, describes both the risk management framework (formerly referred to as certification and accreditation) and the concept of integrated organizationwide risk management.

The NRC Risk Management Program Needs Improvement

In order to evaluate the agency's risk management program, Carson Associates reviewed NRC policies, procedures, and guidance specific to risk management and the risk management framework. We also reviewed the annual security control testing (ASCT) report for the agency's common controls, as risk management strategy (PM-8), the security authorization process (PM-10), and mission/business process definition (PM-11), are provided at the agency level for all NRC information systems.

The agency has established and is maintaining a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, the agency has not developed an organizationwide risk management strategy in accordance with Government policies.

3.2.1 Risk Management Program

NIST SP 800-37, Revision 1, introduces the concept of integrated organizationwide risk management. The three-tiered approach to risk management addresses risk-related concerns at (i) the organization level (Tier 1 – Governance), (ii) the mission and business process level (Tier 2 – Information and Information Flows), and (iii) the information system level (Tier 3 – Environment of Operation) (see Figure 1). Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level.

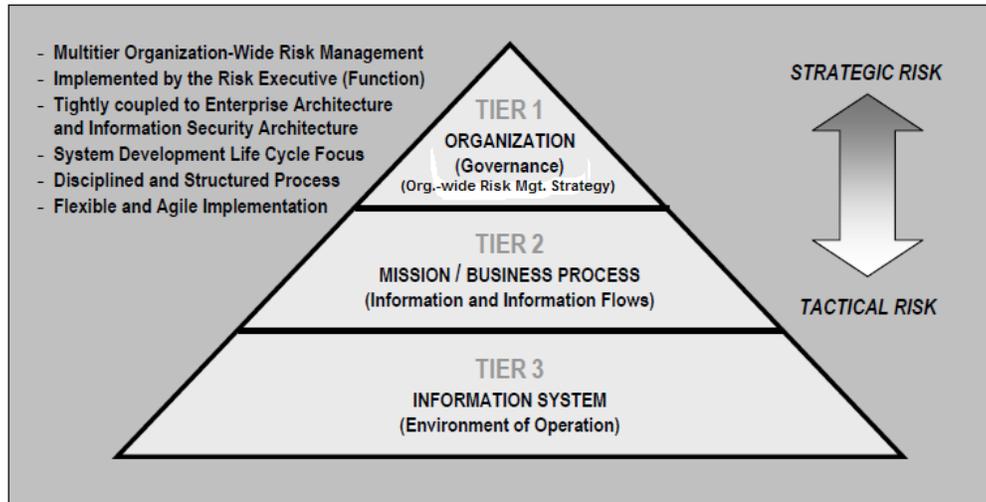


Figure 1: Tiered Risk Management Approach (source: NIST SP 800-37, Revision 1)

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, provides additional guidance for developing and implementing an integrated, organizationwide program for managing information security risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation and use of Federal information systems. This publication describes appropriate governance structures for providing oversight for the risk management activities conducted by an organization and further expands on the role of the risk executive (function).

Documented Policies and Procedures

The agency's risk management program includes documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process. MD and Handbook 12.5 describe the agency's IT security program, including aspects of risk management. This policy states that information security protections shall be commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems that are operated, maintained, or sponsored by the agency. It states that security risks must be managed in a way that complements and does not unnecessarily impede agency business operations. By understanding risks and implementing an appropriate level of cost-effective

controls, NRC can significantly reduce risk and potential loss. MD and Handbook 12.5 define organizational responsibilities for implementing the agency's IT security program, including risk management. MD and Handbook 12.5 require security plans to include a strategy for risk management and that significant risks should be identified, along with responsibilities and mitigation strategies to reduce the security risks. MD and Handbook 12.5 also describe the process for identifying risk for an automated information system.

MD and Handbook 2.8, *Project Management Methodology (PMM)*, and the agency's PMM Web site include policies and procedures for ensuring that IT investments are planned, built, selected, managed, and evaluated to maximize the value and minimize the risks of those investments in accordance with Federal statutes and regulations. The PMM states risk management must be applied to all IT projects throughout the life cycle and that risks to project success must be identified early and managed before they become problems.

The PMM also includes an IT capital planning and investment control (CPIC) program to ensure management of IT investments through the research, selection, control, and evaluation phases of the investment life cycle. Participants in the CPIC program provide governance at the organizational level to ensure risk is addressed from an organizational perspective. These participants include the Executive Director for Operations (EDO) and Chief Financial Officer (CFO), the Chief Information Officer (CIO), the Program Review Committee, the IT/Information Management (IM) Senior Advisory Council (ITSAC), the IT/IM Strategic Planning Group (ITSPG), the IT/IM Business Council (ITBC), the Enterprise Configuration Control Board, and the Deputy Executive Directors for Operations (DEDO) as the Designated Approving Authorities (DAA).

The NRC CPIC process, a component of the PMM, addresses NRC mission business needs, processes, and process impacts for information security risk. Business sponsors must identify business needs, business processes, business process impacts, alignment with the NRC Strategic Plan and Enterprise Architecture, and security considerations in the Vision and Business Case documents. These documents must be reviewed and assessed by the ITBC and approved by the CIO or the Office of Information Services (OIS) in order to receive approval to proceed to the next phase of the CPIC and PMM processes.

The first step of the risk management framework, categorize, documents information protection needs arising from the defined business processes. Information types are mapped to the Business Area, Line of Business, and Sub-Function from the Federal Enterprise Architecture Business Reference Model listed in the Business Case and associated impact levels are assessed in accordance with NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, Volumes I and II, and Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*. Security categorizations are reviewed and must be approved by CSO in order for the project to proceed to the next step in the risk management framework.

Risk is addressed from an information system perspective as part of the NRC Risk Management Framework (RMF), which focuses on identifying information system risk throughout the system development life cycle. The RMF is guided by risk decisions at the organizational perspective

and the mission/business perspective. For example the selection of agencywide common controls at the organizational level guides the implementation of system level controls. The agency conducts system-specific risk assessments as part of the security assessment and authorization process and updates them as part of the agency's continuous monitoring process.

Communication of Risk

System specific risks are reported via quarterly POA&M updates and security assessment briefings to office directors and DAAs. Mission/business specific risks are communicated at the monthly ITBC meeting, semiannual ITSAC meeting, and monthly senior executives meetings. The CIO briefs the Chief Information Security Officer (CISO) and other Office Directors on organizational level risks semi-annually during the ITSAC meeting. Senior officials are also briefed on threat activity on a regular basis by appropriate personnel. The briefings occur at least monthly. Senior officials are briefed by the CISO, OIS Security Operations, the CSO FISMA Compliance and Oversight Team, and CSO Cyber Situational Awareness, Analysis, and Response Team.

NRC Has Not Developed an Organizationwide Risk Management Strategy

NIST SP 800-53, control PM-9, Risk Management Strategy, requires organizations to (i) develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems and (ii) implement that strategy consistently across the organization. While the agency has a governance structure in place at the organizational level to ensure risk is addressed from an organizational perspective, it has not developed or implemented an organizationwide risk management strategy in accordance with government policies.

RECOMMENDATION

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

1. Develop and implement an organizationwide risk management strategy that is consistent with NIST SP 800-37 and NIST SP 800-39.

3.2.2 Risk Management Framework

NIST SP 800-37, Revision 1, also provides guidelines for applying the RMF, which provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle (see Figure 2). The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive, dissemination of updated threat and risk information to authorizing officials and information system owners). The RMF replaces the process formerly known as certification and accreditation.

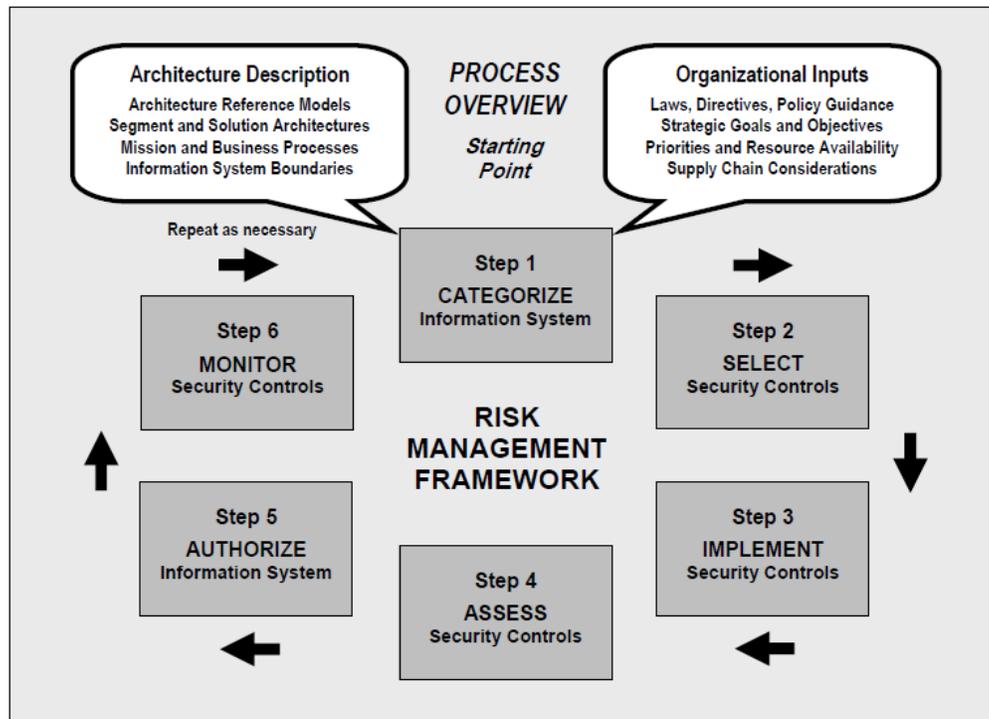


Figure 2: Risk Management Framework (source: NIST SP 800-37, Revision 1)

NIST SP 800-37, Revision 1, describes the process of applying the RMF to Federal information systems and includes a set of well-defined tasks for completing each step of the framework. The document also describes the various roles and responsibilities of key participants in the organization's risk management process (e.g., risk executive (function), authorizing official, authorizing official designated representative, chief information officer, senior information security officer, enterprise architect, information security architect, information owner/steward, information system owner, common control provider, information system security officer, and security control assessor).

Security *authorization* is the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations.

Documented Policies and Procedures

The NRC risk management program includes documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process, specifically the agency's risk management framework policies and procedures. The NRC RMF and Authorization Process describes the process for applying the NIST SP 800-37 risk management framework to secure NRC systems, including the steps

required to obtain IT system authorization and authorization for IT systems, applications, laptops, services, and facilities.

The CSO Web site, specifically the Certification and Accreditation Deliverables page is in the process of being updated for consistency with the new RMF process and the PMM Web site will be updated to point to the RMF process. The PMM Web site includes workflows for the security assessment and authorization 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 RMF artifacts. The PMM Web site also includes guidance on the use of common and inheritable controls.

In order to determine if the agency's risk management framework is consistently implemented, Carson Associates reviewed the security assessment and authorization documents for the three systems selected for evaluation during the FY 2011 independent evaluation and found that the documents 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. We also found that security assessment reports are in accordance with Government policies; accreditation boundaries for agency information systems are defined in accordance with Government policies; and security authorization packages contain a system security plan, security assessment report, and POA&M in accordance with Government policies. Carson Associates also reviewed the security categorizations, security plans, and authorization to operate memoranda for all agency systems and found that (1) all major applications and general support systems have been categorized in accordance with NRC policy, (2) security plans have been developed or updated in accordance with NRC policy, and (3) all agency systems have a current authorization to operate.

All Major Applications and General Support Systems Have Been Categorized in Accordance with NRC Policy

The agency has completed or updated security categorizations for all major applications and general support systems, including those operated by a contractor or other organization on the behalf of the agency.

Security Plans Have Been Developed or Updated in Accordance with NRC Policy

The agency completed or updated security plans for all of the agency's 22 operational systems and for both contractor systems.

All Agency Systems Have a Current Authorization To Operate

The agency continued to make significant progress in assessing and authorizing its systems. In FY 2011, the agency completed security assessment and authorization of two new agency systems, and completed security assessment and re-authorization of two existing agency systems, and one existing contractor system. As of the completion of fieldwork for FY 2011, all 22 operational NRC information systems and both systems used or operated by a contractor or other organization on behalf of the agency had a current authorization to operate.

3.3 Configuration Management (Question 2)

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 NRC Security Configuration Management Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's security configuration management program, Carson Associates reviewed:

- Configuration management processes and procedures located on the NRC PMM Web site.
- Security assessment and authorization documents for the three systems selected for evaluation during the FY 2011 independent evaluation.
- ASCT results for agency and contractor systems, specifically the results for controls related to configuration management.

The agency has established and is maintaining a configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines. However, Carson Associates found that configuration management procedures are not consistently implemented. Specifically, (i) standard baseline configurations are not implemented on some NRC systems; (ii) software compliance assessment procedures are not consistently implemented; and (iii) vulnerability remediation and patch management procedures are not consistently implemented.

Documented Policies and Procedures

The agency's security configuration management program includes documented policies and procedures for configuration management. MD and Handbook 2.8 describe the agency's project management policy, which includes configuration and change management. The purpose of change management is to identify configuration items, manage baselines and changes to configuration items, audit changes to configuration items, and define and manage baselines of configuration items. Central configuration is considered a key supporting element for the PMM and office directors and regional administrators are required to keep the NRC's central configuration management system (Rational ClearCase) current.

The PMM Web site provides additional details on the PMM and includes descriptions and a work breakdown structure for each phase of the PMM life cycle. Planning a project's configuration management and change control is part of the first phase of the life cycle. Managing change requests and baselines is part of all phases of the life cycle. To support

configuration management and change control, the PMM Web site also provides several tools and documents including additional guidance and instructions on using the agency's central configuration management system, as well as training presentations and exercises. The agency also has a template for developing system-specific configuration management plans.

NRC also maintains an agency Master Configuration Management Plan on the PMM Web site that defines the configuration management procedures for NRC projects from inception to decommissioning. The Master Configuration Management Plan outlines the use of the agency's central configuration management system for version control and change management for all software projects at NRC.

Federal Desktop Core Configuration (FDCC)/United States Government Configuration Baseline (USGCB) Secure Configurations

The agency's security configuration management program includes a process for ensuring, FDCC/USGCB secure configuration settings for Windows-based components are fully implemented, and any deviations from FDCC/USGCB baseline settings are fully documented. 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 and are configured to FDCC standards during computer build-out. 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.

The agency's continuous monitoring process requires hardening checks at least on an annual basis, if not more frequently depending on the system sensitivity level. The continuous monitoring process also requires each office and its respective systems to undergo continuous monitoring reviews, conducted by the CSO, once per fiscal year. During the review, CSO support personnel verify the FDCC settings for the office's laptops and standalone PCs.

In addition, the agency has deployed SCAP scanning tools to verify that the agency is compliant with FDCC during security assessment and authorization. Offices and regions are required to ensure all laptops belonging to their office/region comply with FDCC standards by performing scans with approved SCAP tools. NRC conducts monthly FDCC compliance checks on all networked computers using nCircle. Non-networked computers, such as standalone laptops, are scanned for FDCC compliance using ThreatGuard.

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.

Changes to Hardware and Software Configurations

The agency's security configuration management program includes documented proposed or actual changes to hardware and software configurations. The NRC PMM process requires all requests for changes to be submitted via Change Requests, which are submitted by certain NRC end users, Business Sponsors, or Task Order Managers through the agency's central configuration management tool. The PMM process also describes the steps for reviewing and responding to Change Requests, making iterative updates to the configuration baseline, and reporting configuration status. Configuration Management Boards convene at least quarterly and for emergency changes and coordinate and provide oversight for configuration change control activities.

To determine if the agency documents proposed or actual changes to configuration settings, Carson Associates reviewed security test and evaluation (ST&E) results for the three systems selected for evaluation in FY 2011, and ASCT results for agency and contractor systems, specifically the test results for CM-3 control, Configuration Change Control. This control requires organizations to authorize, document, and control changes to the information system. The agency's security configuration management program includes documented proposed or actual changes to hardware and software configurations. ASCT and ST&E found this control to be in place for all three systems selected for evaluation in FY 2011 and for all but two of the remaining NRC systems. For one of those systems, the control is partially in place. For that system, the agency has documented proposed or actual changes to configuration settings, but is currently not auditing those activities.

Standard Baseline Configurations Are Not Implemented on Some NRC Systems

The agency's security configuration management program includes standard baseline configuration definitions. The CSO has developed standard baseline configurations for software (e.g., operating systems, databases, browsers), hardware (e.g., Blackberries, thumb drives, laptops, printers), and other technologies (e.g., Web 2.0, YouTube, Twitter, Citrix) in use at the agency. CSO-defined configuration standards are used as system baseline configurations for any information system that stores, transmits/receives, or processes NRC information. In the absence of CSO configuration standard, the agency allows Defense Information Systems Agency (DISA) standards, checklists, and guidance to be used. In the absence of both CSO and DISA configuration information, the agency allows Center for Information Security (CIS) benchmarks to be used.

To determine if standard baseline configurations are implemented on NRC systems, Carson Associates reviewed ST&E results and vulnerability assessment reports prepared in support of ST&E for the three systems selected for evaluation in FY 2011. We also reviewed ASCT results for agency and contractor systems, specifically the test results for CM-2, Baseline Configuration, and CM-6, Configuration Settings. CM-2 requires organizations to develop, document, and

maintain under configuration control, a current baseline configuration of the information system, and CM-6 requires organizations to establish and document mandatory configuration settings for information technology products employed within an information system.

Despite the agency's requirement to use standard baseline configurations for any information system that stores, transmits/receives, or processes NRC information, baseline configurations are not implemented on some NRC systems. Vulnerability scanning performed as part of ST&E (conducted in support of the security assessment and authorization process) and ASCT identified numerous vulnerabilities that demonstrate non-compliance with required baseline configurations in several systems – both legacy systems and a new system. These are vulnerabilities that have been identified by the agency as actual weaknesses requiring remediation and are being tracked on the agency's POA&M. In addition, ASCT found that configuration baselines and settings had not been documented for one system and that the system was not configured in compliance with agency requirements, even though this system has been in operation for many years. While a number of these vulnerabilities have been corrected since initially identified, there are still several on the POA&M that have not been corrected, including several identified by the agency during their 4th quarter FY 2010 scan of one system that have yet to be remediated. The number of actual weaknesses requiring remediation related to the implementation and documentation of standard baseline configurations indicates the agency needs to improve its configuration management procedures to ensure the NRC standard baselines are consistently implemented for all systems and to ensure baseline configurations are documented for all systems.

RECOMMENDATIONS

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

2. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure standard baseline configurations are implemented for all systems.
3. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure baseline configurations are documented for all systems.

Software Compliance Assessment Procedures Are Not Consistently Implemented

The agency's configuration management program includes procedures for assessing software for compliance with baseline configurations. The agency performs a vulnerability assessment before a system is connected to the NRC production environment, and during ST&E performed as part of security assessment and authorization. Testing includes vulnerability scans, penetration tests, and hardening checks using a variety of tools, such as nCircle, CIS benchmarks, the CORE Impact penetration testing tool, DISA Gold Disk, NRC hardening guides, Nessus vulnerability scanner, and the Secutor Prime vulnerability scanner.

The agency's continuous monitoring process requires networked-based scans and wireless scans, at least on an annual basis if not more frequently, depending on the system sensitivity level.

System owners must provide evidence of periodic scanning to the CSO on the 15th of November, February, May, and August.

To determine if software compliance assessment procedures are consistently implemented, Carson Associates reviewed ST&E results and vulnerability assessment reports prepared in support of ST&E for the three systems selected for evaluation in FY 2011. We also reviewed ASCT results for agency and contractor systems, specifically the test results for CM-6, Configuration Settings, and RA-5, Vulnerability Scanning. CM-6 requires organizations to establish and document mandatory configuration settings for information technology products employed within an information system and RA-5 requires organizations to scan for vulnerabilities in information systems and hosted applications.

Despite agency requirements and existing procedures for assessing for compliance with baseline configurations, software compliance assessment procedures are not consistently implemented. For one system, ASCT found no evidence any vulnerability scans had been done on that system, even though the system has been in operation for many years. For another system that also has been in operation for many years, ST&E performed in support of the re-authorization of the system found that while vulnerability scans are conducted continuously as part of the agency's continuous monitoring program, additional scans conducted during the ST&E found numerous vulnerabilities on servers at headquarters and in the regions. The ST&E testers' finding, as stated in their report, was that "either not all the segments were included in the automated continuous monitoring scans and/or scan results from nCircle were not accessible to appropriate personnel for prompt remediation." The fact that recent ST&E and ASCT activities have identified a number of vulnerabilities in systems that have been operational for many years indicates the agency needs to improve its configuration management procedures to ensure software compliance assessments, including vulnerability scans, are performed as required and to ensure all system components are included in requisite software compliance assessments.

RECOMMENDATIONS

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

4. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure software compliance assessments, including vulnerability assessments, are performed as required: (i) before a system is connected to the NRC production environment, (ii) during security test and evaluation of systems, and (iii) as part of the agency's continuous monitoring environment.
5. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure all system components are included in requisite software compliance assessments.

Vulnerability Remediation and Patch Management Procedures Are Not Consistently Implemented

The agency's configuration management program includes a process for timely remediation of vulnerabilities, including configuration-related vulnerabilities and scan findings, and for the

timely and secure installation of software patches. System owners are required to patch, scan, and check the security of their systems with the rigor and frequency appropriate for the system sensitivity level and to define the frequency for conducting routine patching. NRC requires legitimate vulnerabilities to be remediated in accordance with an organizational assessment of risk and within the following timeframes:

- Within 7 calendar days for critical findings.
- Within 30 calendar days for high risk findings.
- Within 90 calendar days for moderate risk findings.
- Within 120 calendar days for low risk findings.

NRC also requires system owners to ensure automated mechanisms are employed quarterly to determine the state of information system components with regard to flaw remediation.

To evaluate the agency's procedures for vulnerability remediation and patch management, Carson Associates reviewed ST&E results for the three systems selected for evaluation in FY 2011, and ASCT results for agency and contractor systems, specifically the test results for RA-5, Vulnerability Scanning, and SI-2, Flaw Remediation. RA-5 requires organizations to scan for vulnerabilities in information systems and hosted applications and SI-2 requires organizations to identify, report, and correct information system flaws.

Despite the existence of configuration management procedures regarding vulnerability remediation and patch management, vulnerabilities, including configuration-related vulnerabilities, scan findings, and security patch-related vulnerabilities, are not always remediated in a timely manner. ST&E and ASCT of some systems that have been in operation for many years found that a number of vulnerabilities found during previous scans had not been remediated within the timeframes required by the agency. In addition, ST&E of two systems found that servers were missing required upgrades or patches. Both of these systems have been operational for many years as well. ST&E of one system found that many components had never been hardened or scanned in the past and many patches (old and new) had not been installed. ST&E of the other system found similar issues and the ST&E report recommended the agency determine the root causes for not promptly identifying, reporting, and correcting information flaws, as the same problem was encountered during the previous ST&E performed on the system in 2009. The ST&E report also noted that the numerous security patch-related vulnerabilities identified during ST&E may be a result of either the agency's enterprise-wide patching solution not being properly configured to detect missing patches or personnel responsible for these system components not manually requesting the patches from the enterprise-wide patching solution.

The fact that recent ST&E and ASCT activities have identified problems with the timely remediation of vulnerabilities in more than one operational system indicates the agency needs to improve its configuration management procedures to ensure all identified vulnerabilities, including configuration-related vulnerabilities, scan findings, and security patch-related vulnerabilities, are remediated in a timely manner in accordance with the timeframes established by NRC.

RECOMMENDATION

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

6. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure all identified vulnerabilities, including configuration-related vulnerabilities, scan findings, and security patch-related vulnerabilities, are remediated in a timely manner in accordance with the timeframes established by NRC.

3.4 Incident Response and Reporting (Question 3)

FISMA requires agencies to develop, document, and implement an agencywide information security program that includes procedures for detecting, reporting, and responding to security incidents. NIST SP 800-53 requires organizations to (1) implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; (2) track and document information system security incidents; (3) report security incident information to designated authorities; and (4) develop an incident response plan that provides the organization with a roadmap for implementing its incident response capability.

The NRC Incident Response and Reporting Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's security incident reporting program, Carson Associates reviewed NRC policies, procedures, and guidance specific to incident response and reporting. We also reviewed the ASCT report for the agency's common controls, as incident response policies and procedures are provided at the agency level for all NRC information systems, and interviewed personnel responsible for implementing incident response policies and procedures. We determined that the agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Documented Policies and Procedures

The agency's incident response and reporting program includes documented policies and procedures for detecting, responding to, and reporting incidents. MD and Handbook 12.5, Appendix B, formalizes the agency's procedures for monitoring, detecting, reporting, and responding to information systems security incidents. It also provides the requirements and procedures for reporting incidents internally, for reporting to the United States Computer Emergency Readiness Team (US-CERT),⁸ and for reporting to law enforcement. The MD defines the roles and responsibilities for reporting and responding to information systems security incidents.

⁸ The procedures actually reference reporting to the Federal Computer Incident Response Center, which was replaced with the US-CERT when the Department of Homeland Security was established. Newer NRC procedures properly refer to US-CERT.

On May 2, 2008, the agency issued a revised policy on computer security incident response and personally identifiable information (PII) incident response. The policy provides direction for responding to computer security incidents affecting the NRC's systems, networks, and users, as well as PII incidents and will be included in the next revision of MD and Handbook 12.5. The revised policy contains timeframes for responding to 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: Computer Security Office, Office of Information Services, Office of Administration, and Office of Nuclear Security and Incident Response. The policy also specifies when the OIG should be involved in addressing a computer security incident.

In addition to issuing the revised policy on computer security incident response and PII incident response and forming CSIRT, the agency developed the following policies and guidelines related to detecting, reporting, and responding to security incidents. These documents include guidance on reporting incidents internally, reporting incidents to US-CERT, and reporting to law enforcement.⁹

- Information Systems Security Incident Response Procedures, May 11, 2004 (Appendix B from MD and Handbook 12.5).
- CSIRT Responder Guide, Version 2.0, May 20, 2011.
- CSIRT Standard Operating Procedures, Version 2.0, June 30, 2011.

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

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

In order to determine if incident response and reporting procedures are consistently implemented in accordance with Government policies, we reviewed the ASCT report for the agency's common controls. Incident response policies and procedures are provided at the agency level for all NRC information systems. ASCT of all incident response controls found them to be implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the agency.

⁹ 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.

Analysis, Validation, and Documentation of Incidents

The agency's incident response and reporting program includes comprehensive analysis, validation, and documentation of incidents. The agency recently issued the Computer Security Incident Response Plan, CSO-IR PLAN-6001, Version 1.0, June 20, 2011, which provides the NRC plan for responding to computer security incidents affecting NRC's infrastructure, networks, and users. It describes the organization of the NRC incident response capability and is intended to be used by security personnel who are assigned computer security incident response related duties and responsibilities. The NRC Computer Security Incident Response Plan describes the incident handling capability and guidance for preparation, detection and analysis, containment, eradication, and recovery are included in both the NRC CSIRT Incident Response Responder Guide and CSIRT Test Plan.

Incidents are documented using a CSIRT Incident Report Form and monitored using the CSIRT Incident Response Tracking Sheet and these documents are retained in a centralized location. The CSIRT Incident Report Form and CSIRT Incident Response Tracking Sheet provide detailed information about incidents reported to the CSIRT and allow the CSIRT to maintain records about each incident, monitor the status of incidents, maintain other pertinent information necessary for forensics, and evaluate incident details, trends, and handling.

Reporting to US-CERT and Law Enforcement

The agency's incident response and reporting program includes procedures for reporting to US-CERT within established timeframes. The NRC Computer Security Incident Response Plan states the CSIRT uses the US-CERT Incident Reporting System Web Site as a secure automated mechanism for reporting computer security related incidents. NRC requires NRC staff and contractors to report suspected computer security incidents to the NRC CSIRT via telephone or email within 1 hour of detection. The CSIRT Responders Guide and the CSIRT Standard Operating Procedures specify the types of incidents that must be reported to US-CERT, and the timeframes for reporting each category of incident to US-CERT. The agency's incident response and reporting program includes also includes procedures for reporting to law enforcement within established timeframes. The CSIRT Responder Guide states the CSIRT is responsible for determining if law enforcement and/or OIG involvement is needed. MD and Handbook 12.5 state that when criminal activity is suspected or confirmed, the procedures assign the OIG responsibility for contacting and coordinating the response with law enforcement officials.

Responding To and Resolving Incidents

The agency's incident response and reporting program includes procedures for responding to and resolving incidents in a timely manner, as specified in agency policy or standards, to minimize further damage. The NRC Computer Security Incident Response Plan states the CSIRT prioritizes, monitors, tracks, and coordinates computer security related incidents at NRC. Categories and classes of incidents are defined and appropriate actions to take are included in the NRC CSIRT Standard Operating Procedures and CSIRT Responder Guide. The incident handling capability and guidance for preparation, detection and analysis, containment,

eradication, and recovery are included in both the NRC CSIRT Incident Response Responder Guide and CSIRT Test Plan.

Tracking and Managing Risk in Virtual/Cloud Environments

The agency's incident response and reporting program is capable of tracking and managing risks in a virtual/cloud environment. The NRC does not currently have or make use of "cloud" environments for its systems. The NRC does run a clustered virtualized server environment and proactively tracks and manages risk in that environment in the same manner it does for non-virtualized systems.

Correlating Incidents

The agency's incident response and reporting program is capable of correlating incidents. The agency uses a variety of tools, including firewalls, a variety of filtering tools, scanners, intrusion detection systems, and data loss prevention tools, to detect and respond to cyber security incidents and these tools allow the agency to correlate incidents and perform regular incident correlation activities.

3.5 Security Training (Question 4)

FISMA requires agencies to develop, document, and implement an agencywide information security program that includes security awareness training to information personnel, including contractors and other users of information systems that support the operations and assets of the agency. The security awareness training must inform personnel of information security risks associated with their activities, and their responsibilities in complying with agency policies and procedures designed to reduce these risks. NIST SP 800-53, requires organizations to (1) provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and periodically thereafter; (2) provide role-based security-related training before authorizing access to the system or performing assigned duties, when required by system changes, and periodically thereafter; and (3) document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

The NRC Security Training Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's security training program, Carson Associates reviewed:

- NRC policies, procedures, and guidance specific to security awareness and security training.
- The ASCT report for the agency's common controls, as security awareness and security training policies and procedures are provided at the agency level for all NRC information systems.

- The content of several of the agency's security awareness and specialized security training courses.

We determined that the agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Documented Policies and Procedures

The agency's security training program includes documented policies and procedures for security awareness training. MD and Handbook 12.5 require the agency CIO to ensure through coordination with the Office of Human Resources that NRC employees and contractor staff have appropriate initial and refresher, basics and literacy, and role-based computer security training. The NRC Associate Director for Training and Development, Office of Human Resources is responsible for providing assistance in the development and delivery of appropriate information security awareness and training programs for NRC personnel, ensuring that an information security briefing is included in the initial orientation for new employees, ensuring that employees receive periodic computer security refresher training, including awareness, basics, and literacy instruction, and maintaining records concerning computer security training provided to NRC employees. MD and Handbook 12.5 also require all users of NRC information systems to attend initial indoctrination and annually complete the computer security awareness refresher training.

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

For FY 2011, 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 by August 15, 2011. The self-paced course consisted of three parts. The first part was a general computer security awareness training course developed by another Government agency for Governmentwide use. The second part addressed NRC-specific computer security awareness information and addressed the IT protection of SGI. The third part was a review of the agencywide Rules of Behavior for Authorized Computer Use and acknowledgement. Completion of all three parts 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 part of the training as a companion document to the FY 2011 training.

The agency also routinely issues network announcements on various security topics, including spoofed and fake e-mail messages, social engineering, phishing, and security issues while teleworking. 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.

The agency's security training program also includes documented policies and procedures for training users with significant information security responsibilities. The agency developed an IT Role-Based Training plan that states the requirement for training for those with significant IT responsibilities, the type of training expected for each role, and frequency of training per role. System owners are responsible for using the training plan procedures to address the training needs of personnel with IT roles.

The CSO developed four role-based courses for senior level managers/executive, IT managers/system owners, and ISSOs, and for System Administrators. The CSO also provides commercial training as resources permit. The CSO IT Security Role-Based Training Web page provides examples of commercially available training and additional commercial-related IT security training can be found on iLearn.

In order to determine if security awareness training procedures are consistently implemented in accordance with Government policies, we reviewed the ASCT report for the agency's common controls as security awareness training procedures are provided at the agency level for all NRC information systems. ASCT of all awareness and training controls found them to be implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the agency.

Security Training Status Tracking

The agency's security training program includes identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training. Each office is responsible for ensuring all users are entered into the iLearn system, which is used to track completion of the annual security awareness training. The CSO's IT Security Training Web site includes a link to a Web page showing the completion rate for the computer security awareness training by office. As of August 16, 2011, the agency had a 98-percent completion rate.

The agency's security training program also includes identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training. With regard to IT security roles-based training, CSO tracks completion dates in the IT Security Roles Training Requirements spreadsheet, as individuals notify CSO of attendance and at the end of the year through a data call requiring training coordinators to update the spreadsheet with training attendance information for their staff.

3.6 POA&M (Question 5)

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. NIST SP 800-53 requires organizations to implement a process for ensuring that POA&Ms for the security program and the associated organizational information systems are maintained and document the remedial information security actions to

mitigate risk to organizational operations and assets, individuals, other organizations, and the Nation. It requires organizations to develop a POA&M for each information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and it also requires organizations to update existing POA&Ms periodically based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

The NRC POA&M Program Needs Improvement

In order to evaluate the agency's POA&M program, Carson Associates reviewed NRC policies, procedures, and guidance specific to POA&Ms. We also reviewed the ASCT report for the agency's common controls, as POA&M policies and procedures are provided at the agency level for all NRC information systems, and analyzed the agency's POA&Ms from Q1 FY 2011 through Q4 FY 2011. We determined that the agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses.

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

As in previous independent evaluations, Carson Associates also found that (1) POA&Ms do not include all known security weaknesses, (2) initial target remediation dates are still often missed, and (3) POA&Ms are not updated in a timely manner. These issues are primarily due to the manual process that was used for managing and updating the POA&Ms up until Q4 FY2011 and should improve over time as the agency continues to use Xacta. The OIG will continue to monitor the agency's POA&M procedures and its use of Xacta throughout the following year's independent evaluation to determine whether these issues have been resolved.

Documented Policies and Procedures

The agency's POA&M program includes documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation. MD and Handbook 12.5 require the system owner/sponsor to ensure that a POA&M is developed, implemented, and maintained to track the major weaknesses that have been identified for office-sponsored information systems. Each office is required to regularly update the CIO on its progress in correcting system weaknesses in order to enable the CIO to provide the agency's quarterly FISMA update report to OMB.

The NRC POA&M Process was issued by the CSO to ensure quality assurance is emphasized and includes a process for conducting independent verification and validation of POA&Ms to assure their adequacy as part of the security assessment review process. Additionally, CSO acquired additional contract support to assist in establishing a compliance review process in which CSO will review security documentation, conduct vulnerability scanning, and meet with

each system owner on an annual basis to verify the status of remediation efforts, assess the comprehensiveness of planned corrective actions, and validate the accuracy of tasks, responsibilities, and milestones for each outstanding weakness. These activities take place quarterly, targeting approximately 25 percent of the overall number of POA&Ms. The POA&M process was also briefed to various system owners and internal forums.

In addition, the NRC POA&M Process includes procedures 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. The agency adds any new weaknesses identified from various sources including OIG audits and reports, Government Accountability Office (GAO) audits, internal control reviews, ASCT, ST&E, information security program reviews, critical infrastructure protection vulnerability assessments, risk assessments, penetration tests, security information assessment recommendations, security assessment reports, quarterly scanning, vulnerability assessment reports, and confirmed security incidents.

Tracking, Prioritizing, and Remediating Weaknesses

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 actions items such as ASCT 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. 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. After months of research and evaluation the CSO picked Xacta, which was purchased in the second half of 2009, as the agency's tool for automating the POA&Ms. The agency began using Xacta for automating the POA&Ms beginning with Q4 FY2011.

The more specific corrective actions associated with the security assessment and authorization process (e.g., corrective actions resulting from risk assessments, ST&E, and ASCT) are tracked in Rational[®] ClearQuest^{®10} as change requests using the PMM process for change management. All corrective actions arising from the security control testing process and from vulnerability scans are imported into Rational ClearQuest. A corrective action plan is generated directly from Rational ClearQuest. System owners are responsible for remediation of each corrective action within the timeframes specified in the corrective action plan.

The agency's new POA&M procedures require corrective actions to be ranked based upon on the most critical security weaknesses and their impact on the agency's mission and that 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. Xacta provides a severity code

¹⁰ Rational ClearQuest is an IBM software package used for software change management.

field for identifying the risk impact level of a weakness and a rank field for setting the relative priority for weaknesses within each risk level category.

Adequate Resources

The agency's POA&M program ensures adequate resources are provided for correcting weaknesses. System owners are responsible for incorporating resources required for completing corrective actions and ongoing security costs into the total amount allocated for security and to ensure general weakness descriptions noted in CPIC documentation correspond to the weaknesses documented in the corresponding POA&M. If additional hardware, software, services, or staffing are required, the POA&M should identify the cost of the resources required, even if already included in the organization budget. Xacta provides a field for listing the resources required for corrective action. System owners can report whether weakness mitigation resources are Funded, Unfunded, or will be Reallocated.

POA&Ms Do Not Include All Known Security Weaknesses

The agency POA&M procedures require weaknesses identified from various sources to be added to the appropriate program-level or system-level POA&M. These sources include OIG audits and reports, GAO audits, internal control reviews, ASCT, ST&E, information security program reviews, critical infrastructure protection vulnerability assessments, risk assessments, penetration tests, security information assessment recommendations, security assessment reports, quarterly scanning, vulnerability assessment reports, and confirmed security incidents.

The agency POA&M procedures also require new weaknesses to be added to the POA&M within 15 days of discovery. However, not all IT-related weaknesses were added to the POA&Ms as required by agency policy.

- POA&Ms do not include all IT-related weaknesses identified in OIG audits. For example, an OIG report on one of the agency's systems (NSTS) was issued in August 2010; however, only one of the five recommendations from the report was added to the POA&M. In September 2010, the OIG issued a report on the use of wireless at the agency. Only 3 of the 18 recommendations from that report were added to the POA&M.
- Recommendations from a recent GAO audit on securing wireless networks were not added to the POA&M. While the agency may have procedures for tracking findings from GAO audits at the agency level, these recommendations were IT-related and should also be tracked on the agency's POA&Ms.
- None of the recommendations from the FY 2011 contingency plan testing have been added to the POA&Ms.
- Not all of the weaknesses identified during the FY 2011 ASCT have been added to the POA&Ms.

Initial Target Remediation Dates Are Still Often Missed

Carson Associates analyzed the POA&Ms for the three systems selected for evaluation in FY 2011 to determine if target remediation dates are met. Two of the three systems had at least one

weakness that was closed more than 5 months after the scheduled completion date. One system had eight weaknesses that were closed over a year after their scheduled completion dates. Two of the three systems had half of their open weaknesses overdue.

POA&Ms Are Not Updated in a Timely Manner

Carson Associates analyzed all four of the agency's FY 2011 POA&M submissions to OMB to determine whether POA&Ms are updated in a timely manner. We found multiple instances of POA&M items being reported closed more than 3 months after they were actually closed. In addition, we found multiple instances of the agency not counting weaknesses as closed when they had been closed by the OIG prior to the cutoff date for POA&M reporting.

3.7 Remote Access (Question 6)

OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, requires agencies to allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access and to use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity. NIST SP 800-53, control AC-17, Remote Access, requires organizations to authorize, monitor, and control all methods of remote access to their information systems.

The NRC Remote Access Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's remote access program, Carson Associates reviewed NRC policies, procedures, and guidance related to remote access. We also reviewed the ASCT report for the agency's infrastructure system for control AC-17, Remote Access. This control requires organizations to authorize, monitor, and control all methods of remote access to the information system. We determined that the agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Documented Policies and Procedures

On June 26, 2008, the agency issued the NRC Computer Security Information Protection Policy to address requirements specified OMB Memorandum M-06-16, and M-06-19, *Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency IT Investments*. The policy includes the requirement for remote access to any system that processes non-public NRC information to be constrained by a "time-out" function that requires re-authentication after 30 minutes of inactivity.

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

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

NRC provides centralized remote access via a component of its IT infrastructure system. After remote access through the centralized component, users have the same access to the network, NRC information, and NRC information systems as if they were logged into the network locally. The agency monitors remote access via a variety of mechanisms. At the agency level, this control was found to be in place, with the exception of enhancement two, which requires the use of cryptography to protect the confidentiality and integrity of remote access sessions.

Cryptography is not used to protect the confidentiality and integrity of remote access sessions via dial-up. The agency has conducted a cost-benefit analysis to determine the feasibility of implementing a compliant solution and found that it is not cost justifiable due to a limited number of select users having dialup access. The agency will be requesting a waiver for this enhancement.

3.8 Identity and Access Management Program (Question 7)

NIST SP 800-53 includes several controls related to identity and access management, including the following:

- AC-2, Account Management – Requires organizations to manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts, and to review system accounts at least annually.
- IA-1, Identification and Authentication Policy and Procedures – Requires organizations to develop, disseminate, and periodically review/update (i) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance and (ii) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls.
- IA-2, User Identification and Authentication – Requires information systems to uniquely identify and authenticate users (or processes acting on behalf of users). Also specifies requirements for the use of multifactor authentication.
- IA-3, Device Identification and Authentication – Requires information systems to identify and authenticate specific devices before establishing a connection.
- IA-4, Identifier Management – Requires organizations to manage user identifiers by (i) uniquely identifying each user, (ii) verifying the identity of each user, (iii) receiving authorization to issue a user identifier from an appropriate organization official, (iv) issuing the user identifier to the intended party, (v) disabling the user identifier after an organization-defined period of inactivity, and (vi) archiving user identifiers.

The NRC Identity and Access Management Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's identity and access management program, Carson Associates reviewed:

- NRC policies, procedures, and guidance related to identity and access management.
- Security assessment and authorization documents for the three systems selected for evaluation during the FY 2011 independent evaluation, specifically controls related to identity and access management.
- The ASCT report for the agency's common controls and the agency's infrastructure system.

We determined that the agency has established and is maintaining an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Carson Associates found minor deviations from the agency's established identity and access management procedures. Specifically, some enhancements for account management, identification and authentication, and identifier management are not in place for a few of the agency's systems. The agency's continuous monitoring process ensures that these issues are identified, tracked on the agency's POA&M, and remediated if possible. For those controls that cannot be implemented, the agency's RMF allows system owners to formally request approval from the DAA to deviate from existing IT security requirements due to limitations (e.g., technical, business process, etc.).

Documented Policies and Procedures

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

The agency has also issued several procedures and standards related to identity and access management, including the following:

- CSO-PROC-1323, NRC Procedure to Submit a Request for IT Hardware Security Approval.
- CSO-STD-0001, NRC Strong Password Standard.
- CSO-STD-2006, User Access Management Standard.
- CSO-STD-2007, Network Access Control Standard.

To determine if identity and access management procedures are consistently implemented, Carson Associates reviewed ST&E results for the three systems selected for evaluation in FY 2011, the test results for the agency's common controls, and the agency's infrastructure system and found the following minor deviations:

- AC-2 – Test results indicate this control is in place for all systems reviewed with the exception of enhancement 3, which requires information systems to automatically disable inactive accounts after an organization-defined time period. NRC requires inactive accounts to be disabled after no more than 35 days of inactivity. Two of the systems are requesting a waiver for this enhancement based on the average usage of the systems. One system is also not able to implement enhancement 4, which requires information systems to automatically audit account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals. This system is not able to automatically notify appropriate individuals of account actions. This system is also requesting a waiver for this enhancement.
- IA-1 – Test results indicate the agency has developed and disseminated an agencywide identification and authentication policy for all systems; however, the organization does not review/update the policies and procedures annually as required by NRC. The overall procedures in MD and Handbook 12.5 have not been updated since 2003. MD and Handbook 12.5 are currently undergoing an update.
- IA-2 – Test results indicate this control is in place for all systems with the exception of enhancements related to multi-factor authentication certain types of access. Resolution of these issues is dependent on completion of the agency's implementation of the HSPD-12 Personal Identity Verification card.
- IA-3 – This control is in place for all systems reviewed.
- IA-4 – Test results indicate this control is in place for all but one of the systems reviewed. This control requires systems to disable user identifiers after an organization-defined time period of inactivity. NRC requires user identifiers to be disabled after no more than 35 days of inactivity. This system is requesting a waiver for this enhancement based on the average usage of the systems.

3.9 Continuous Monitoring Management (Question 8)

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.

At the agency level, NIST SP 800-53 requires agencies to (i) manage (i.e., document, track, and report) the security state of organizational information systems through security authorization processes, (ii) designate individuals to fulfill specific roles and responsibilities within the organizational risk management process, and (iii) fully integrate the security authorization processes into an organizationwide risk management program. The last step of the security authorization process (the RMF) is monitor.

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

The NRC Continuous Monitoring Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's enterprisewide continuous monitoring program, Carson Associates reviewed NRC policies, procedures, and guidance related to continuous monitoring. We also reviewed the continuous monitoring activities performed for all of the agency's operational systems, including contractor systems. We determined that the agency has established and is maintaining an enterprisewide continuous monitoring program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Documented Policies and Procedures

CSO-PROS-1323, US NRC Agencywide Continuous Monitoring Program, provides direction for NRC continuous monitoring activities and describes the process for annual continuous monitoring reviews, related roles and responsibilities and evaluation criteria. Continuous monitoring reviews are conducted on each office and its respective systems once per fiscal year to provide System Owners and the Designed Approving Authorities with insight into the agencywide IT security posture.

Once a year, the agency EDO issues a memorandum and risk management instructions requiring system owners to perform continuous monitoring activities required for FISMA. System owners are required to take the following actions:

1. Perform an annual contingency plan test and submit an updated contingency plan and contingency plan test report to the CSO.
2. In coordination with CSO, perform ASCT of NRC information systems and ensure that all ASCT reports are submitted in a timely fashion.
3. For systems owned and/or operated by other agencies or contractors (e.g., e-Government systems), obtain a memorandum from the owning/operating agency/contractor confirming the completion of annual FISMA requirements and Authorization to Operate status.
4. Conduct periodic patching and scanning.
5. Update all security-related documentation (e.g., System Security Plans) in accordance with NRC requirements.
6. Proactively track and mitigate open POA&M weaknesses identified during the course of ongoing security activities and provide timely submission of quarterly POA&M updates.

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

Contingency plan testing is discussed in Section 3.10. Procedures for the oversight of contractor systems are discussed in Section 3.11. The agency's security assessment and authorization process, including security plan updates, is discussed in Section 3.2.2. The agency's POA&M program is discussed in Section 3.6. ASCT is discussed below.

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

Of the agency's 24 operational systems, 3 were authorized to operate in the past fiscal year or underwent a full security control assessment as part of a re-authorization and, therefore, did not require additional ASCT. The remaining 18 agency systems and both contractor systems required ASCT. As of the completion of fieldwork for FY 2011, ASCT was completed for the 18 agency systems and 2 contractor systems that required ASCT.

3.10 Contingency Planning (Question 9)

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.

The NRC Business Continuity/Disaster Recovery Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's enterprisewide business continuity/disaster recovery program, Carson Associates reviewed NRC policies, procedures, and guidance related to contingency planning. We also reviewed the contingency plans and contingency plan test reports for all of the agency's operational systems, including contractor systems. We determined that the agency has established and is maintaining an enterprisewide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Documented Policies and Procedures

MD and Handbook 12.5 state 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 CSO and OIS procedures also require annual contingency plan testing for all major applications and general support systems, including generating a contingency plan test report.

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

The Executive Director for Operations issued a memorandum in December 2010 requiring system owners to perform continuous monitoring activities required for FISMA, including completing annual contingency plan testing of all major applications and general support systems. System owners were required to perform an annual contingency plan test and submit to the CSO an updated contingency plan and contingency plan test report. Testing completion dates must not exceed 1 year from when the last test was performed. The instructions accompanying the memorandum also specify the types of contingency plan tests appropriate for low, moderate, and high system impact levels.

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

As of the completion of fieldwork for FY 2011, contingency plan testing¹¹ was completed for all 22 of the agency's operational NRC information systems and for both contractor systems for which NRC has direct oversight. In addition, all operational NRC information systems and all contractor systems have current contingency plans.

3.11 Contractor Systems (Question 10)

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.¹²

¹¹ Any testing performed between October 1, 2010, and the completion of fieldwork would be considered as FY 2011 test results.

¹² 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.

The NRC Contractor Oversight Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's program to oversee contractor systems, Carson Associates reviewed:

- NRC policies, procedures, and guidance related to contractor oversight.
- NRC's inventory of systems.
- Agreements such as memoranda of understanding (MOU), Interconnection Service Agreements, and contracts.
- Annual security control test reports, certification and accreditation documents, contingency plans, and contingency plan test reports for both contractor systems for which NRC has direct oversight.
- Documentation the agency obtained from the seven e-Government systems used by the agency confirming the completion of annual FISMA requirements and Authorization to Operate status.

We determined that the agency has established and is maintaining a contractor oversight program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.

Documented Policies and Procedures

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 authorized to operate prior to processing any sensitive NRC information or connecting to the NRC infrastructure and must undergo ASCT and annual contingency plan testing. Contractor systems are also required to undergo re-authorization 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, ASCT, 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.

The agency currently has no agency systems residing in a public cloud but does utilize several services that are considered software as a service. The agency's risk management framework describes both system and service types used to characterize NRC information systems and the authorization requirements for each type. Authorization types are either authorization to operate or authorization to utilize (ATU). ATUs are issued for services such as those provided by other

Federal organizations (e.g., e-Government systems) or by private contractors (e.g., software as a service). The NRC risk management framework also describes the authorization requirements for social media including public Web 2.0 Web sites owned and operated by external third-party providers such as YouTube and Facebook.

Agency Oversight of Contractor Systems Meets FISMA Requirements

As of the completion of fieldwork for FY 2011, both contractor systems for which NRC has direct oversight had a current authorization to operate and both have met NRC requirements for continuous monitoring, including ASCT, security plan updates, and annual contingency plan testing and contingency plan update. The agency also has documentation demonstrating all seven e-Government systems used by the agency have completed of annual FISMA requirements and have a current authorization to operate.

3.12 Security Capital Planning (Question 11)

At the organizational level, NIST SP 800-53 requires organizations to (1) ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement, (2) employ a business case/Exhibit 300/Exhibit 53 to record the resources required, and (3) ensure that information security resources are available for expenditure as planned.

At the system level, NIST SP 800-53 requires organizations to (1) include a determination of information security requirements for the information system in mission/business process planning; (2) determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process; and (3) establish a discrete line item for information security in organizational programming and budgeting documentation.

The NRC CPIC Program Is Generally Consistent with FISMA Requirements, OMB Policy, and Applicable NIST Guidelines

In order to evaluate the agency's capital planning and investment program, Carson Associates reviewed NRC policies, procedures, and guidance specific to capital planning. We also reviewed the ASCT report for the agency's common controls, specifically control PM-3, Information Security Resources, as this control is provided at the agency level for all NRC information systems. We determined that the agency established and maintains a security capital planning and investment program for information security.

Documented Policies and Procedures

The agency's CPIC program includes documented policies and procedures to address information security in the capital planning and investment control process. MD and Handbook 2.8 describe the agency's project management policy. The purpose of the PMM is to establish an IT investment process that facilitates the effective selection, implementation, management, and evaluation of IT investments throughout their entire life cycle. The PMM also includes an IT CPIC program to ensure management of IT investments through the research, selection, control, and evaluation phases of the investment life cycle. The CPIC process is a key component of

PMM and consists of four phases at NRC: research, select, control, and evaluate. MD and Handbook 2.8 include a mapping of the four CPIC phases to the six PMM phases. The PMM Web site provides additional details on CPIC and includes descriptions and process flow diagrams for each CPIC phase.

To support the CPIC process, the PMM Web site provides several tools and documents including an Automated CPIC Process System User Guide. The PMM also has templates for various CPIC artifacts including project screening forms, Vision and Business Case documents, System Requirements Specifications, and Project Management Plans.

In order to determine if CPIC procedures are consistently implemented, we reviewed the ASCT report for the agency's common controls, specifically control PM-3, Information Security Resources, as this control is provided at the agency level for all NRC information systems. ASCT of this control found it to be implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the agency. We reviewed the agency's budget year 2012 Exhibit 300s for the agency's major investments, and the agency's budget year 2012 Exhibit 53 and found them to be consistent with the agency's CPIC program.

Information Security Requirements as Part of CPIC

The agency's CPIC program includes information security requirements as part of the capital planning and investment process. All capital planning and investment requests are required to include the resources needed to implement the information security program. The Exhibit 300 has several key sections on spending, including security and privacy.

Business Case/Exhibit 300/Exhibit 53

The agency's CPIC program employs a business case/Exhibit 300/Exhibit 53 to record the information resources required and to establish a discrete line item for information security. The Exhibit 300 has several key sections on spending, including security and privacy. The Exhibit 53 for budget year 2012 includes a line item for computer security. This investment includes providing IT security compliance tracking; updates and support for staff security awareness and ISSO training, IT security training for management, security incident response, conducting the annual FISMA reviews, and independent IT security testing. The Exhibit 53 also includes a line item for IT Strategic Management. This investment includes support for the CPIC process, IT budget reporting, and project control, and ensures integrity and security of systems and vendor products, compliance with project management standards, and technical assessment of hardware and software prior to purchase. In addition, each major investment on the Exhibit 53 has a column for reporting IT security costs.

Information Security Resources

The agency's CPIC program ensures that information security resources are available for expenditure as planned. The CPIC process requires project managers to coordinate all security-related activities directly through the Senior Information Technology Security Officer for the

CSO FISMA Compliance and Oversight Team to ensure that the project meets all IT security requirements necessary for security assessment and authorization of the system, and with the Senior Information Technology Security Officer for the CSO Cyber Situational Awareness, Analysis, and Response Team, to ensure the system infrastructure architecture meets security technical configuration standards before implementation.

The annual EDO memorandum and instructions on performing IT security risk management activities include cost estimates for annual IT risk management tasks, including contingency plan testing, contingency plan updates, vulnerability scans, security hardening checks, Web application security assessments, and wireless scanning. The CSO has budgeted for the performance of ASCT to relieve system owners of any additional burden.

[Page intentionally left blank]

4 Consolidated List of Recommendations

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

1. Develop and implement an organizationwide risk management strategy that is consistent with NIST SP 800-37 and NIST SP 800-39.
2. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure standard baseline configurations are implemented for all systems.
3. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure baseline configurations are documented for all systems.
4. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure software compliance assessments, including vulnerability assessments, are performed as required: (i) before a system is connected to the NRC production environment, (ii) during security test and evaluation of systems, and (iii) as part of the agency's continuous monitoring environment.
5. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure all systems components are included in requisite software compliance assessments.
6. Revise existing configuration management procedures to include performance measures and/or monitoring procedures to ensure all identified vulnerabilities, including configuration-related vulnerabilities, scan findings, and security patch-related vulnerabilities, are remediated in a timely manner in accordance with the timeframes established by NRC.

[Page intentionally left blank]

5 Agency Comments

At an exit conference on November 3, 2011, agency officials agreed with the report's findings and recommendations and provided some editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[Page intentionally left blank]

Appendix. OBJECTIVE, SCOPE, AND METHODOLOGY

OBJECTIVE

The objective of this review was to perform an independent evaluation of the NRC's implementation of FISMA for FY 2011.

SCOPE

The evaluation focused on reviewing the agency's implementation of FISMA for FY 2011. We conducted this evaluation at NRC headquarters from April 2011 through September 2011. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. The evaluation included assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines, and a review of information security policies, procedures, and practices of a representative subset of the agency's information systems, including contractor systems and systems provided by other Federal agencies. Throughout the evaluation, evaluators were aware of the potential for fraud, waste, or misuse in the program.

METHODOLOGY

To conduct the independent evaluation, the team met with agency staff responsible for implementing the agency's information system security program, reviewed security assessment and authorization 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.

The evaluation work was conducted by Jane M. Laroussi, CISSP and Virgil Isola, CISSP, from Richard S. Carson & Associates, Inc.