# EVALUATION REPORT

Independent Evaluation of
NRC's Implementation of the
Federal Information Security Management
Act for Fiscal Year 2008

OIG-08-A-18 September 26, 2008

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

September 26, 2008

MEMORANDUM TO: R. William Borchardt
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT FOR FISCAL YEAR 2008 (OIG-08-A-18)

Attached is the Office of the Inspector General's (OIG) audit report titled, *Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act For Fiscal Year 2008.*

The report presents the results of the subject audit. Agency comments provided at the September 16, 2008, exit conference have been incorporated, as appropriate, into this report.

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

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

Attachment: As stated

Electronic Distribution

Edward M. Hackett, Executive Director, Advisory Committee on Reactor
Safeguards/Advisory Committee on Nuclear Waste and Materials
E. Roy Hawkens, Chief Administrative Judge, Atomic Safety and
Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jim E. Dyer, Chief Financial Officer
Margaret M. Doane, Director, Office of International Programs
Rebecca L. Schmidt, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
Bruce S. Mallett, Deputy Executive Director for Reactor
and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Waste, Research,
State, Tribal, and Compliance Programs, OEDO
Darren B. Ash, Deputy Executive Director for Corporate Management
and Chief Information Officer, OEDO
Vonna L. Ordaz, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Cynthia A. Carpenter, Director, Office of Enforcement
Charles L. Miller, Director, Office of Federal and State Materials
and Environmental Management Programs
Guy P. Caputo, Director, Office of Investigations
Thomas M. Boyce, Director, Office of Information Services
James F. McDermott, Director, Office of Human Resources
Michael R. Johnson, Director, Office of New Reactors
Michael F. Weber, Director, Office of Nuclear Material Safety and Safeguards
Eric J. Leeds, Director, Office of Nuclear Reactor Regulation
Brian W. Sheron, Director, Office of Nuclear Regulatory Research
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
Luis A. Reyes, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Elmo E. Collins, Jr., Regional Administrator, Region IV

# Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2008

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

**September 19, 2008**

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

[Page intentionally left blank]

# EXECUTIVE SUMMARY

## BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an annual independent evaluation of an agency's information security program[1] and practices to determine their effectiveness. This evaluation must include testing the effectiveness of information security policies, procedures, and practices for a representative subset of the agency's information systems. FISMA requires the annual evaluation to be performed by the agency's Inspector General (IG) or by an independent external auditor.

Office of Management and Budget (OMB) memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated July 14, 2008, requires the agency's IG to complete the OMB FISMA Reporting Template for IGs (referred to by OMB as Section C). That template is submitted to OMB as part of the agency's annual FISMA report and is included as Appendix B to this report.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on August 31, 2008. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible.

## PURPOSE

The objective of this review was to perform an independent evaluation of the Nuclear Regulatory Commission's (NRC) implementation of FISMA for fiscal year (FY) 2008.

## RESULTS IN BRIEF

### Program Enhancements and Improvements

Over the past 6 years, NRC has made improvements to its information system security program and continues to make progress in implementing the recommendations resulting from previous FISMA evaluations. In order to meet FISMA requirements as they relate to information technology (IT) security, the Commission, on November 14, 2007, approved the establishment of the Computer Security Office (CSO). The new office reports to the Deputy Executive Director for Information Services (DEDIS) and Chief Information Officer (CIO) and is headed by the Chief Information Security Officer (CISO). The CISO plans, directs, and oversees the implementation of a comprehensive, coordinated, integrated, and cost-effective NRC IT security program, consistent with

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

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

Two significant deficiencies were identified in the FY 2007 FISMA independent evaluation. Both of these significant deficiencies have been addressed in FY 2008.

- In FY 2007, only 2 of the 30 operational NRC information systems had a current certification and accreditation, and only 4 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation. As of the completion of fieldwork for FY 2008, 14 of the 28 most risk-significant operational NRC information systems had a current certification and accreditation, and 8 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation. While only 50 percent of the operational NRC information systems have a current certification and accreditation, Carson Associates no longer considers this a significant deficiency due to the significant progress the agency has made during the past fiscal year. The FY 2007 FISMA independent evaluation found that in the past 2 years the agency had completed certification and accreditation of only two NRC systems and one contractor system for which NRC has direct oversight. In FY 2008, the agency completed certification and accreditation of 12 NRC systems and 1 contractor system for which NRC has direct oversight – more than four times the number completed in the previous 2 fiscal years.[2] The certification and accreditation of two systems is nearing completion, and the agency has stated in its fourth quarter FY 2008 FISMA submission to OMB that it plans to complete certification and accreditation of the remaining systems in FY 2009.
- In FY 2007, annual contingency plan testing was still not being performed for all systems. As of the completion of fieldwork for FY 2008, the agency had completed annual contingency plan testing for all agency systems and all contractor systems for which NRC has direct oversight.

In addition to making significant progress on the two significant deficiencies identified in FY 2007, the agency has accomplished the following since the FY 2007 FISMA independent evaluation:

- All major applications and general support systems have been categorized in accordance with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- The agency completed annual security control testing for all agency systems and for all contractor systems for which NRC has direct oversight.

[2] One system was issued a limited authorization to operate that expires after 1 year. The agency is currently making the corrections specified by the designated approving authority and is recertifying and re-accrediting the system.

- The agency completed or updated security plans for 14 of the agency's 28 operational systems and for all contractor systems for which NRC has direct oversight.
- The agency has made progress in implementing the provisions of OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII).* For example, on September 19, 2007, NRC issued the *NRC Personally Identifiable Information Breach Policy* and the *NRC Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers*. Section 3.7.2 provides additional details on the agency's progress in implementing the provisions of the OMB memorandum.

### Program Weaknesses

While the agency has made significant improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified four information system security program weaknesses. Two are repeat findings from the FY 2007 independent evaluation, and two are new.

- The NRC inventory does not identify interfaces between systems (new finding).
- The quality of the agency's plans of action and milestones (POA&M) needs improvement (repeat finding).
- Not all Windows XP and Vista systems[3] have implemented Federal Desktop Core Configuration (FDCC) security settings (new finding).
- The agency lacks procedures for ensuring employees with significant IT security responsibilities receive security training (repeat finding).

## RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve NRC's information system security program and implementation of FISMA. Recommendations are made in this report for the new findings only. Recommendations for the repeat findings were made in prior reports and completion of those findings is being tracked through the Office of the Inspector General (OIG) followup process. A consolidated list of recommendations appears on page 33 of this report.

## AGENCY COMMENTS

At an exit conference on September 16, 2008, agency officials agreed with the report's findings and recommendations and provided 2 editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[3] Windows XP and Vista are operating systems produced by Microsoft.

[Page intentionally left blank]

## ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| BPIAD | Business Process Improvement and Applications Division |
| Carson Associates | Richard S. Carson and Associates, Inc. |
| CIO | Chief Information Officer |
| CIS | Center for Internet Security |
| CISO | Chief Information Security Officer |
| CSIRT | Computer Security Incident Response Team |
| CSO | Computer Security Office |
| DEDIS | Deputy Executive Director for Information Services |
| DISA | Defense Information Systems Agency |
| FDCC | Federal Desktop Core Configuration |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| FY | Fiscal Year |
| IATO | Interim Authorization to Operate |
| IG | Inspector General |
| IRSD | Information and Records Services Division |
| ISS | Information System Security |
| IT | Information Technology |
| MD | Management Directive |
| 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 |
| P2P | Peer-to-Peer |
| P3P | Platform for Privacy Preferences Project |
| PIA | Privacy Impact Assessment |
| PII | Personally Identifiable Information |
| POA&M | Plan of Action and Milestones |
| SP | Special Publication |
| UPI | Unique Project Identifier |
| US-CERT | United States Computer Emergency Readiness Team |

[Page intentionally left blank]

## TABLE OF CONTENTS

**Executive Summary** ........ i
**Abbreviations and Acronyms** ........ v

**1 Background** ........ 1
**2 Purpose** ........ 1
**3 Findings** ........ 1
**3.1 FISMA Systems Inventory (Question 1)** ........ 4
All Major Applications and General Support Systems Have Been Categorized in Accordance With FIPS 199 ........ 5
Security Categorizations Reflect the Information Types That Reside on the Systems ........ 5
**3.2 FISMA Systems Inventory (Question 2)** ........ 6
Annual Contingency Plan Testing Was Completed for All Agency Systems and All Contractor Systems for Which NRC Has Direct Oversight ........ 7
**3.3 Evaluation of Agency Oversight of Contractor Systems (Question 3a)** ........ 8
Agency Oversight of Contractor Systems Meets FISMA Requirements ........ 8
Agency Continues To Have Difficulty in Obtaining Documentation That Demonstrates e-Government Systems Meet FISMA Requirements ........ 9
**3.4 Evaluation of Quality of Agency System Inventory (Questions 3b-3f)** ........ 10
FINDING A – The NRC Inventory Does Not Identify Interfaces Between Systems (New Finding) ........ 11
**3.5 Evaluation of Agency POA&M Process (Question 4)** ........ 11
FINDING B – The Quality of the Agency's POA&Ms Still Needs Improvement (Repeat Finding) ........ 13
NRC Has Made Progress in Correcting Weaknesses Reported on Its POA&Ms ........ 14
**3.6 IG Assessment of the Certification and Accreditation Process (Question 5)** ........ 15
NRC Has Made Significant Progress in Certifying and Accrediting Its Systems ........ 18
NRC Has Completed or Updated Security Plans for 14 of the Agency's 28 Operational
Systems and for All Contractor Systems for Which NRC Has Direct Oversight ........ 18
The Agency's Certification and Accreditation Process and the Documents Completed Using the New Procedures are Consistent with NIST Guidance ........ 18
NRC Has Completed Annual Security Control Testing for All Agency Systems and for All Contractor Systems for Which NRC Has Direct Oversight ........ 20
**3.7 IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process (Questions 6-7)** ........ 21
**3.7.1 Privacy Impact Assessment Process** ........ 21
**3.7.2 Progress in Implementing OMB M-07-16** ........ 23
**3.8 Configuration Management (Question 8)** ........ 25
**3.8.1 Configuration Policy and Common Security Configurations** ........ 25
**3.8.2 Federal Desktop Core Configuration (FDCC)** ........ 26

FINDING C – Not All Windows XP and Vista Systems Have Implemented FDCC Security Settings (New Finding) ........ 27

3.9 Incident Reporting (Question 9) ........ 29

3.10 Security Awareness Training (Question 10) ........ 29

FINDING D – Agency Still Developing Procedures for Ensuring Employees With Significant IT Security Responsibilities Receive Security Training (Repeat Finding) ....... 30

3.11 Collaborative Web Technologies and Peer-to-Peer File Sharing (Question 11) ........ 31

3.12 E-Authentication Risk Assessments (Question 12) ........ 31

4 Consolidated List of Recommendations ........ 33

5 Agency Comments ........ 35

## Appendices

Appendix A. SCOPE AND METHODOLOGY ........ 37

Appendix B. FY 2008 OMB FISMA REPORTING TEMPLATE FOR IGs ........ 39

## List of Tables

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

Table 3-2. Number and Percentage of Systems Reviewed That Are Certified and Accredited, for Which Security Controls Have Been Tested and Reviewed in the Past Year, and for Which Contingency Plans Have Been Tested in Accordance With Policy by FIPS 199 Risk Impact Level ..... 6

## 1 Background

On December 17, 2002, the President signed the E-Government Act of 2002, which included FISMA.[4] 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 IG or by an independent external auditor.

OMB memorandum M-08-21 requires the agency's IG to complete the OMB FISMA Reporting Template for IGs. That template is submitted to OMB as part of the agency's annual FISMA report.

Richard S. Carson and Associates, Inc. (Carson Associates), performed an independent evaluation of NRC's implementation of FISMA for FY 2008. This report presents the results of that independent evaluation. Carson Associates also prepared the OMB FISMA Reporting Template for IGs for inclusion in the agency's annual FISMA report. The OMB FISMA Reporting Template for IGs is included as Appendix B to this report.

This report reflects the status of the agency's information system security program as of the completion of fieldwork on August 31, 2008. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible.

## 2 Purpose

The objective of this review was to perform an independent evaluation of NRC's implementation of FISMA for FY 2008. Appendix A contains a description of the evaluation scope and methodology.

## 3 Findings

Over the past 6 years, NRC has made improvements to its information system security program and continues to make progress in implementing the recommendations resulting from previous FISMA evaluations. In order to meet FISMA requirements as they relate to IT security, the Commission, on November 14, 2007, approved the establishment of the CSO. The new office reports to the DEDIS and CIO and is headed by the CISO. The CISO plans, directs, and oversees the implementation of a comprehensive, coordinated, integrated, and cost-effective NRC IT security program, consistent with applicable laws; regulations; Commission, Executive Director for Operations, and CIO direction; management initiatives; and policies.

The CSO was established to serve as the focal point for IT security and to provide vision, leadership, and oversight in developing, promulgating, and implementing an end-to-end NRC IT

[4] 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.

security strategy. The CSO is divided into three core areas: Cyber Situational Awareness, Analysis, and Response Team; FISMA Compliance and Oversight Team; and Policy, Standards, and Training Team. The CSO provides IT security oversight responsibility, coordinates the overall agency IT security program, develops policies and procedures, and provides assistance with security reviews, assessments, and plans to those offices requiring it. The organizational changes became effective November 25, 2007. The DEDIS/CIO acted as the CISO until that position was filled effective March 16, 2008.

Two significant deficiencies were identified in the FY 2007 FISMA independent evaluation. Both of these significant deficiencies have been addressed in FY 2008.

- In FY 2007, only 2 of the 30 operational NRC information systems had a current certification and accreditation, and only 4 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation. As of the completion of fieldwork for FY 2008, 14 of the 28 most risk-significant operational NRC information systems had a current certification and accreditation, and 8 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation. While only 50 percent of the operational NRC information systems have a current certification and accreditation, Carson Associates no longer considers this a significant deficiency due to the significant progress the agency has made during the past fiscal year. The FY 2007 FISMA independent evaluation found that in the past 2 years the agency had completed certification and accreditation of only two NRC systems and one contractor system for which NRC has direct oversight. In FY 2008, the agency completed certification and accreditation of 12 NRC systems and 1 contractor system for which NRC has direct oversight – more than four times the number completed in the previous 2 fiscal years. The certification and accreditation of two systems is nearing completion, and the agency has stated in its fourth quarter FY 2008 FISMA submission to OMB that it plans to complete certification and accreditation of the remaining systems in FY 2009.
- In FY 2007, annual contingency plan testing was still not being performed for all systems. As of the completion of fieldwork for FY 2008, the agency had completed annual contingency plan testing for all agency systems and all contractor systems for which NRC has direct oversight.

In addition to making significant progress on the two significant deficiencies identified in FY 2007, the agency has also accomplished the following since the FY 2007 FISMA independent evaluation:

- All major applications and general support systems have been categorized in accordance with FIPS 199.
- The agency completed annual security control testing for all agency systems and for all contractor systems for which NRC has direct oversight.
- The agency completed or updated security plans for 14 of the agency's 28 operational systems and for all contractor systems for which NRC has direct oversight.

- The agency has made progress in implementing the provisions of OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII)*. For example, on September 19, 2007, NRC issued the *NRC Personally Identifiable Information Breach Policy* and the *NRC Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers*. Section 3.7.2 provides additional details on the agency's progress in implementing the provisions of the OMB memorandum.

While the agency has made significant improvements in its information system security program and has made progress in implementing the recommendations resulting from previous FISMA evaluations, the independent evaluation identified four information system security program weaknesses. Two are repeat findings from the FY 2007 independent evaluation, and two are new.

- The NRC inventory does not identify interfaces between systems (new finding).
- The quality of the agency's POA&Ms needs improvement (repeat finding).
- Not all Windows XP and Vista systems have implemented FDCC security settings (new finding).
- The agency lacks procedures for ensuring employees with significant IT security responsibilities receive security training (repeat finding).

Recommendations are made in this report for the new findings only. Recommendations for the repeat findings were made in prior reports, and completion of those findings is being tracked through the OIG followup process.

The following sections present the detailed findings from the independent evaluation and are organized based on the OMB FISMA Reporting Template for IGs, which can be found in Appendix B of this report. Each major section corresponds to a question or set of questions from the template. Findings are presented in the sections to which they are relevant.

## 3.1 FISMA Systems Inventory (Question 1)

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

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

| | Agency Systems | | Contractor Systems | | Total Number of Systems (Agency and Contractor Systems) | |
|---|---|---|---|---|---|---|
| **FIPS 199 Risk Impact Level** | **Number** | **Number Reviewed** | **Number** | **Number Reviewed** | **Total Number** | **Total Number Reviewed** |
| **High** | 11 | 1 | 1 | 0 | 12 | 1 |
| **Moderate** | 17 | 2 | 9 | 0 | 26 | 2 |
| **Low** | 0 | 0 | 1 | 1 | 1 | 1 |
| **Not Categorized** | 0 | 0 | 0 | 0 | 0 | 0 |
| **Total** | 28 | 3 | 11 | 1 | 39 | 4 |

NRC has a total of 28 operational systems that fall under FISMA reporting requirements.[5] Of the 28, 15 are general support systems,[6] and 13 are major applications.[7] As required by FISMA, Carson Associates selected a subset of NRC systems for evaluation during the FY 2008 FISMA independent evaluation.

NRC has a total of 11 systems operated by a contractor or other organization on behalf of the agency (9 major applications and 2 general support systems). Of the 11, 8 are operated by other Federal agencies, 1 is operated by a federally funded research and development center, and 2 are operated by private contractors. NRC has direct oversight of three of these systems. Oversight of the remaining eight systems is the responsibility of the Federal agencies operating the systems. Therefore, the IGs of those agencies are responsible for evaluating those systems.

[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.

As required by FISMA, Carson Associates selected for evaluation a subset of contractor systems for which NRC has direct oversight during the FY 2008 FISMA independent evaluation.

## Security Categorization – Background

FIPS 199 requires all Federal agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The security categorization of an information system is conducted by first categorizing all information types[8] resident on the information system. The security category of an information type is established by determining the potential impact (i.e., low, moderate, high) for each security objective (i.e., confidentiality, integrity, availability) associated with the particular information type.

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

## All Major Applications and General Support Systems Have Been Categorized in Accordance With FIPS 199

The FY 2007 independent evaluation found that the majority of NRC major applications and general support systems had not been categorized in accordance with FIPS 199. As of the completion of fieldwork, the agency has completed categorizations for all major applications and general support systems, including those operated by a contractor or other organization on the behalf of the agency. The agency completed security categorizations for 13 agency systems and 6 contractor systems in FY 2008. The agency also updated the security categorization for one contractor system in FY 2008.

## Security Categorizations Reflect the Information Types That Reside on the Systems

The FY 2007 independent evaluation also found that security categorizations for some systems did not consistently reflect the information types that reside on the systems. The agency has started the process of reviewing and correcting security categorizations and has developed security categorization review criteria as a supplement to the existing security categorization procedures. To evaluate the agency's progress in resolving the problem, Carson Associates reviewed the security categorizations for three agency systems and two contractor systems. We compared the information types enumerated in the security categorizations with the primary information types for those systems as identified in the agency's Exhibit 53[9] for FY 2007 and

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

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

with updated unique project identifiers (UPI)[10] provided by the agency. Carson Associates found that the security categorizations for four of the five systems reflect the primary business area, primary line of business, and/or primary sub-function of those systems as indicated on the Exhibit 53 or in the updated UPI.

## 3.2 FISMA Systems Inventory (Question 2)

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

**Table 3-2. Number and Percentage of Systems Reviewed That Are Certified and Accredited, for Which Security Controls Have Been Tested and Reviewed in the Past Year, and for Which Contingency Plans Have Been Tested in Accordance With Policy by FIPS 199 Risk Impact Level**

|  | # Systems Reviewed That Are Certified and Accredited |  | # Systems Reviewed for Which Security Controls Have Been Tested and Reviewed in the Past Year |  | # Systems Reviewed for Which Contingency Plans Have Been Tested in Accordance With Policy |  |
|---|---|---|---|---|---|---|
| **FIPS 199 Risk Impact Level** | **Total Number** | **Percent of Total** | **Total Number** | **Percent of Total** | **Total Number** | **Percent of Total** |
| **High** | 1 | 100% | 1 | 100% | 1 | 100% |
| **Moderate** | 2 | 100% | 2 | 100% | 2 | 100% |
| **Low** | 1 | 100% | 1 | 100% | 1 | 100% |
| **Not Categorized** | 0 | 100% | 0 | 100% | 0 | 100% |
| **Total** | 4 | 100% | 4 | 100% | 4 | 100% |

This section reports on the number of agency and contractor systems that were reviewed that are certified and accredited and for which security controls have been tested and reviewed in the past year. Section 3.6 of this report discusses the assessment of the agency's certification and accreditation process in detail and includes the certification and accreditation status and the annual security control testing status of all agency and contractor systems.

[10] The UPI is a 17-digit line code used to uniquely identify IT investments on an Exhibit 53. Each investment identified in an agency's portfolio must have a unique UPI.

## Contingency Plan Testing – Background

FISMA requires agencies to develop plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, *Contingency Planning Guide for Information Technology Systems*, states that contingency plans should be tested at least annually and when significant changes are made to the information system, supported business process(es), or the contingency plan. Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, states that the NRC shall comply with the NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, IT risk assessments, and IT contingency plans) and other applicable NIST automated information security guidance for IT security processes, procedures, and testing. MD 12.5 also states that IT contingency plans for major applications and general support systems shall be tested each year. A live test provides the best indication of the adequacy of a contingency plan test. If a live test cannot be conducted due to operational constraints, a simulated test may be conducted in lieu of the live test. NRC Information Systems Security (ISS) and Office of Information Services (OIS) procedures also require annual contingency plan testing for all major applications and general support systems, including generating a contingency plan test report.

## Annual Contingency Plan Testing Was Completed for All Agency Systems and All Contractor Systems for Which NRC Has Direct Oversight

On November 8, 2007, the CIO sent the agency a request for contingency plan schedules that included a requirement to complete contingency plan testing no later than June 30, 2008. The request also noted that if a system is owned by another agency, then the other agency is responsible for the contingency plan testing; however, NRC must acquire a memorandum from the other agency stating that it has completed its annual contingency plan test in accordance with FISMA. This memorandum must also be received by June 30, 2008.

The FY 2005, FY 2006, and FY 2007 FISMA independent evaluations found that annual contingency plan testing was not being performed for all systems. The lack of annual contingency plan testing was reported as a significant deficiency in the FY 2006 and FY 2007 FISMA independent evaluation reports. In FY 2007, only 5 of the 30 operational NRC information systems and 2 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had their contingency plans tested.

As of the completion of fieldwork for FY 2008, contingency plan testing[11] was completed for all 28 operational NRC information systems and for the 3 contractor systems for which NRC has direct oversight. The agency also received notification from the Federal agencies responsible for eight additional contractor systems that contingency plan testing was completed in FY 2008 for those systems.

[11] Any testing performed between September 1, 2007, and the completion of fieldwork would be considered as FY 2008 test results.

## 3.3 Evaluation of Agency Oversight of Contractor Systems (Question 3a)

| OMB Requirement | OIG Response |
|---|---|
| *3.a. The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.* | *Almost Always (96-100% of the time)* |

### Oversight of Contractor Systems – Background

FISMA requires agencies to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (1) information collected or maintained by or on behalf of the agency or (2) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.[12]

NRC defines two types of systems that are operated by a contractor or other organization on behalf of NRC – e-Government systems and contractor systems. An e-Government system is a system that processes NRC information and is operated and maintained by another Federal agency, and a contractor system is a system that processes NRC information and is operated and maintained by a contractor. NRC requires all e-Government and contractor systems to be certified and accredited prior to processing any sensitive NRC information or connecting to the NRC infrastructure, and for contractor systems, also requires the same annual security requirements and recertification and re-accreditation requirements as NRC systems.

NRC has a total of 11 systems operated by a contractor or other organization on behalf of the agency. Of the 11, 8 are considered e-Government systems and 3 are considered contractor systems. NRC has direct oversight of the three contractor systems. Oversight of the eight e-Government systems is the responsibility of the Federal agencies operating the systems.

### Agency Oversight of Contractor Systems Meets FISMA Requirements

In previous FISMA independent evaluations, Carson Associates found that oversight of contractor systems was lacking. In FY 2007, of the four contractor systems for which NRC has direct oversight,[13] only one had a current certification and accreditation and met all NRC requirements for contractor systems.

As of the completion of fieldwork for FY 2008, two of the three contractor systems for which NRC has direct oversight had a current certification and accreditation. All three had their

[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.

[13] NRC removed one of the four contractor systems for which they have direct oversight from its inventory. This system was consolidated into the local area network/wide area network general support system and is no longer reported as a separate system.

security controls tested and reviewed in the past year and had completed annual contingency plan testing.

## Agency Continues To Have Difficulty in Obtaining Documentation That Demonstrates e-Government Systems Meet FISMA Requirements

In previous FISMA independent evaluations, Carson Associates found that the agency was not maintaining documentation that demonstrates e-Government systems meet FISMA requirements. The agency has been working with the offices to assist in acquiring the required documentation for e-Government; however, according to the agency, some of the other Federal agencies have been unwilling to provide documentation that demonstrates their systems meet FISMA requirements.

The agency continues to have difficulty in obtaining documentation that demonstrates e-Government systems meet FISMA requirements. The following is a summary of the status of documentation for e-Government systems in use at NRC.

- The agency has received documentation from the Federal agencies responsible for six e-Government systems stating that those systems have a current certification and accreditation. One Federal agency has not responded regarding the certification and accreditation status of its system, and one Federal agency system has an expired certification and accreditation.
- The agency has received documentation from the Federal agencies responsible for four e-Government systems stating that those systems have had their security controls tested and reviewed in the past year. Two Federal agencies have not responded regarding the annual security control testing for the three systems for which they are responsible, and one Federal agency system is currently undergoing a recertification and re-accreditation, but a new authorization to operate has not been issued. Subsequent to the completion of fieldwork, the agency received documentation from a Federal agency responsible for two e-Government systems stating those systems have had their security controls tested and reviewed in the past year.
- The agency has received notification from the Federal agencies responsible for all eight e-Government systems stating that those systems have completed annual contingency plan testing.

In its fourth quarter FY 2008 FISMA report to OMB, the agency stated that next year it will remove the e-Government systems from the NRC inventory of reportable systems. The agency will continue to track e-Government systems in its inventory database, but will not be reporting to OMB the status of those systems' certification and accreditation, annual security control testing, or annual contingency plan testing. This should be the responsibility of the Federal agencies that own the systems. Reporting by the agencies that use e-Government systems provided by other Federal agencies is duplicative.

## 3.4 Evaluation of Quality of Agency System Inventory (Questions 3b-3f)

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

### Agency System Inventory – Background

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

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

## FINDING A – The NRC Inventory Does Not Identify Interfaces Between Systems (New Finding)

Carson Associates reviewed security plans for eight 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. Despite the fact that the NSICD database schema includes a field for the identification of interfaces between systems, and the data calls include a requirement to identify interfacing systems, Carson Associates found that only one of the eight records reviewed included interface information, and that information was not consistent with the interface information in the system's security plan.

The agency has acknowledged that the interface information in the inventory is incomplete and is currently populating a comment field in the database with interface information. The agency has also stated it is planning to redesign the inventory database schema to ensure interface information can be adequately captured in the future. While the NRC inventory does not identify interfaces between systems as required by FISMA, interface information is documented in both the security plans and risk assessments for the systems reviewed.

### RECOMMENDATIONS

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

1. Update the NRC System Information Control Database to identify all interfaces between systems.
2. Develop and implement procedures to ensure interface information in the NRC System Information Control Database is consistent with interface information in security plans and risk assessments.

## 3.5 Evaluation of Agency POA&M Process (Question 4)

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

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

## Agency POA&M Process – Background

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

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

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

The agency has developed a process for requesting quarterly POA&M updates from system owners, compiling the data into a consolidated source, reviewing it for accuracy, rolling up the information, and reporting it to OMB. Five weeks prior to the quarterly submittal to OMB, the agency sends out a data call to the offices asking them to update the current POA&Ms for their systems and add new weaknesses to the POA&Ms. Three weeks prior to the quarterly submittal to OMB, the agency receives the updated POA&M data from the system owners and enters the data into NSICD. The agency also adds any new weaknesses identified from various sources

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

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

The FY 2007 FISMA independent evaluation found that the quality of the agency's POA&Ms needs improvement. Specifically, Carson Associates found that (1) the metrics submitted to OMB often deviated from the actual POA&Ms, and (2) the agency is not always following OMB and internal NRC POA&M guidance. The FY 2007 FISMA independent evaluation also found that the agency had made minimal progress in correcting weaknesses reported on its POA&Ms.

## FINDING B – The Quality of the Agency's POA&Ms Still Needs Improvement (Repeat Finding)

As in previous independent evaluations, Carson Associates found that the quality of the agency's POA&Ms still needs improvement. In assessing the agency's POA&M process, Carson Associates found that (1) the metrics submitted to OMB often deviated from the actual POA&Ms, and (2) the agency is not always following OMB and internal NRC POA&M guidance. Carson Associates also found that the agency is closing weaknesses without sufficient evidence from the system owner. The agency is currently in the process of implementing quality assurance procedures for POA&Ms.

### Metrics Submitted to OMB Deviate From the Actual POA&Ms

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

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

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

As in previous FISMA evaluations, Carson Associates also found that the agency is not always following OMB's POA&M guidance. The agency is also not following NRC internal POA&M guidance. The following are some examples of deviations from OMB and NRC internal POA&M guidance found on the FY 2008 POA&Ms.

- Weaknesses with completion dates over a year old are not always removed from the POA&Ms. OMB guidance[15] states that weaknesses that are no longer undergoing correction and have been completely mitigated for over a year should no longer be reported in the agency POA&M.
- Weaknesses with changes made to scheduled completion dates. OMB guidance states that once an agency has completed the initial POA&M, no changes should be made to the scheduled completion date.

### The Agency Is Closing Weaknesses Without Sufficient Evidence from the System Owners

During our analysis of weaknesses closed during the first quarter FY 2008, we identified nine weaknesses for one system that should not have been closed based on the corrective actions described in the POA&M. We examined the documents referenced in the agency's resolution and found that they did not include the information required to close the weaknesses. We notified the agency and the weaknesses were added back to the POA&M in the fourth quarter of FY 2008.

### Agency Progress in Implementing Quality Assurance Procedures for POA&Ms

In a memorandum to the OIG, the agency stated it has been working on automating the POA&M process by using NSICD to store, process, and generate the POA&Ms. Once the migration from the Excel spreadsheet to the automated process is completed, the agency will draft procedures for the new process. The agency has recently acquired the Environmental Protection Agency's FISMA reporting solution, the Automated System Security Evaluation and Remediation Tracking system, to further automate the POA&M and continuous monitoring processes. The agency currently inputs POA&M data into the tool and has started developing a plan to ensure quality assurance is included in the POA&M process. The plan includes developing a POA&M checklist, using a contractor to perform independent verification and validation of closed POA&M items, and performing quarterly reviews of system and program level POA&Ms.

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

The agency has made progress in correcting weaknesses reported on its POA&Ms. The agency has corrected over 40 percent of its program and system level weaknesses in FY 2008. This is an improvement over FY 2007, as in FY 2007 the agency had only corrected 35 percent of its program level weaknesses and just over 23 percent of its system level weaknesses.

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

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

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

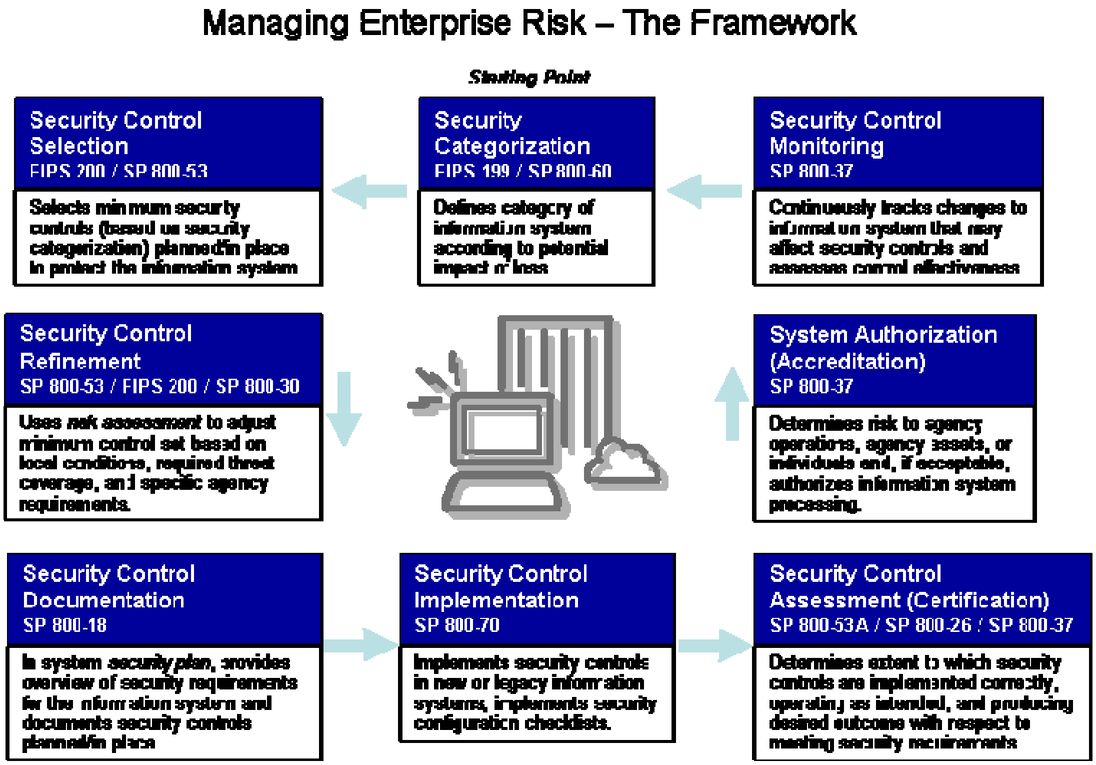
This section reports on Carson Associate's assessment of the agency's certification and accreditation process in detail. To evaluate the agency's certification and accreditation process, Carson Associates evaluated the certification and accreditation documents for the four systems selected for evaluation during the FY 2008 independent evaluation. We reviewed the certification and accreditation process and procedures located on the agency's project management methodology Web site and reviewed accreditation decision memoranda issued by the agency's authorizing official. We also reviewed the agency's annual security control testing process.

We rated the overall quality of the agency's certification and accreditation process as satisfactory because the agency has not completed the certification and accreditation for all agency systems. We did find that the agency has made significant progress in certifying and accrediting its systems, including developing or updating security plans for several systems, and that the agency's certification and accreditation process and the documents completed using the new procedures are consistent with NIST guidance. We also found that the agency has completed annual security control testing for all agency systems and for all contractor systems for which NRC has direct oversight.

### Certification and Accreditation – Background

The security certification and accreditation of information systems is integral to an agency's information security program and is an important activity that supports the risk management process required by FISMA. Information systems under development must be certified and accredited prior to becoming operational. Operational information systems must be recertified and re-accredited every 3 years in accordance with Federal policy,[16] and whenever there is a significant change[17] to the information system or its operational environment.

The following diagram[18] illustrates the key activities, including certification and accreditation, in managing enterprise-level risk, i.e., risk resulting from the operation of an information system. As illustrated in the diagram, NIST has developed several standards and guidelines to support the management of enterprise risk. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, provides guidelines for certification and accreditation.



Managing Enterprise Risk – The Framework

*Starting Point*

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

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

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

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

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

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

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

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

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

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

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

Security *certification* is a comprehensive assessment of the management, operational, and technical security controls[19] that are planned or in place in an information system to determine the extent to which the controls are (1) implemented correctly, (2) operating as intended, and (3) producing the desired outcome with respect to meeting the security requirements for the information system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official[20] to render a security accreditation decision. Security certification can include a variety of assessment methods (e.g., interviewing, inspecting, studying, testing, demonstrating, and analyzing) and associated assessment procedures depending on the depth and breadth of assessment required by the agency.

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

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

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

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

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

- **Denial of Authorization to Operate** – issued if, after assessing the results of the security certification, the authorizing official deems that the risk to agency operations, agency assets, or individuals is unacceptable. The information system is not accredited and should not be placed into operation. If the information system is currently operational, all activity should be halted.

To correct weaknesses identified by the FY 2005 and FY 2006 FISMA independent evaluations, the agency implemented a new certification and accreditation process and developed templates for all certification and accreditation documents, as well as instructions for completing the templates. The new certification and accreditation process was also integrated into the agency's project management methodology.

### NRC Has Made Significant Progress in Certifying and Accrediting Its Systems

The FY 2005, FY 2006, and FY 2007 FISMA independent evaluations found that the majority of NRC information systems were not certified and accredited. The lack of certification and accreditations for the majority of the agency's systems was reported as a significant deficiency in the FY 2006 and FY 2007 FISMA independent evaluation reports. In FY 2007, only 2 of the 30 operational NRC information systems had a current certification and accreditation, and only 4 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation. As of the completion of fieldwork for FY 2008, 14 of the 28 most risk significant operational NRC information systems and 8 of the 11 systems used or operated by a contractor or other organization on behalf of the agency had a current certification and accreditation.

### NRC Has Completed or Updated Security Plans for 14 of the Agency's 28 Operational Systems and for All Contractor Systems for Which NRC Has Direct Oversight

As of the completion of fieldwork for FY 2008, 14 agency systems and the 3 contractor systems for which NRC has direct oversight had new or updated security plans.[21]

### The Agency's Certification and Accreditation Process and the Documents Completed Using the New Procedures are Consistent with NIST Guidance

The FY 2007 independent evaluation found that the agency's new certification and accreditation process was inconsistent with NIST guidance – specifically that certification and accreditation documents completed using the new procedures are inconsistent with NIST guidance. In a memorandum to the OIG, the agency stated it is creating checklists to ensure the quality of certification and accreditation documents. The checklist for security categorizations was completed and issued to the agency in August 2007. The agency also stated it is in the process of developing evaluation criteria checklists for three additional documents. The agency will continue to develop evaluation checklists and distribute them to all system owners and certifying agents. NRC is also currently soliciting feedback from certifying agents and system owners on

[21] The Federal agencies responsible for the eight e-Government systems would be responsible for updating those security plans.

the checklist developed to date. NRC plans to use contract support for reviewing and providing feedback on documents and packages to system owners.

Carson Associates evaluated the certification and accreditation documents for the four systems selected for evaluation during the FY 2008 independent evaluation and found that the documents completed using the new procedures are consistent with NIST guidelines.

### Annual Security Control Testing and Continuous Monitoring – Background

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

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

The FY 2007 FISMA guidance stated that for FY 2007 and beyond agencies are required to use FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, for the specification of security controls, and NIST SP 800-37 and SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, for the assessment of security control effectiveness. The FY 2008 FISMA guidance reiterated this requirement.

The FY 2007 independent evaluation found that the agency did not follow OMB and NIST guidance when conducting its annual security control assessments (formerly referred to as self-assessments). In May 2008, the agency issued a task order for completing annual security control testing for FY 2008. The statement of work specified which agency systems require annual security control testing and which do not. Agency systems that were authorized to operate within the past fiscal year have already had their security controls tested and, therefore, do not require additional annual security control testing. Agency systems that are currently undergoing a certification and accreditation also do not require additional annual security control testing. A total of 14 agency systems were identified for annual security control testing.

The contractor selected to perform the annual security control testing worked with the agency to develop selection criteria for determining which security controls would be tested in FY 2008. The CSO identified a set of 48 core controls to be evaluated for each system specified in the statement of work. Systems scheduled for annual security control testing that are currently operating under an authorization to operate were required to have an additional one-third of the remaining controls selected for evaluation. The additional controls for these systems were selected based on POA&M items resolved in the previous 12 months (or time period following authorization to operate), with additional controls selected from the Access Control, Configuration Management, Contingency Planning, Incident Response, System Maintenance, and System and Services Acquisition control families and/or specific controls deemed necessary by the assessor based on the sensitivity level of the system. For each system scheduled for testing, the contractor prepared an annual security control test plan and a report.

## NRC Has Completed Annual Security Control Testing for All Agency Systems and for All Contractor Systems for Which NRC Has Direct Oversight

As of the completion of fieldwork for FY 2008, annual security control testing was completed for all 14 agency systems identified for annual security control testing. The report for one system is still a draft, but a final report is expected to be issued before the end of the fiscal year. In addition, the security test and evaluations for the three agency systems currently undergoing a certification and accreditation have also been completed. The security test and evaluation reports for those systems are also drafts, but finals are also expected to be issued before the end of the fiscal year.

Annual security control testing is also required for any contractor systems for which NRC has direct oversight. Annual security control testing for e-Government systems is the responsibility of the Federal agencies that operate those systems. NRC has direct oversight of three contractor systems. One contractor system was authorized to operate in FY 2008 and, therefore, did not require additional annual security control testing. Annual security control testing was completed for the other two contractor systems for which NRC has direct oversight.

For the eight e-Government systems in use at NRC, NRC policy is to confirm with the owner agencies that annual security control testing has been completed. The agency has received documentation from the Federal agencies responsible for four e-Government systems stating that those systems had their security controls tested and reviewed in the past year. Two Federal agencies have not responded regarding the annual security control testing for the three systems for which they are responsible, and one Federal agency system is currently undergoing a recertification and re-accreditation, but a new authorization to operate has not been issued. Subsequent to the completion of fieldwork, the agency received documentation from a Federal agency responsible for two e-Government systems stating those systems have had their security controls tested and reviewed in the past year.

## 3.7 IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process (Questions 6-7)

### *3.7.1 Privacy Impact Assessment Process*

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

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

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

MD and Handbook 3.2, *Privacy Act*, requires office directors and regional administrators to ensure that PIAs are prepared and submitted to OIS before developing or procuring IT that collects, maintains, or disseminates personal information about individuals or when initiating a new electronic collection of personal information in identifiable form[22] from 10 or more persons. In accordance with the agency's project management methodology, a PIA is required for all investments at the inception phase of the development life cycle. PIAs are also part of the agency's certification and accreditation process. ISS-01-001, Revision 0, *PIA Procedures,* dated August 30, 2006, requires a PIA (or update of an existing PIA) for each legacy system requiring recertification and re-accreditation.

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

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

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

*6.c. Does the agency have a written policy or process for evaluating changes in business process or technology that the PIA indicate as necessary?*

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

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

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

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

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

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

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

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

MD and Handbook 3.14 is augmented by additional guidance on the agency's internal Web site. The additional guidance includes interface requirements for Web-based software applications, requirements and best practices for Government Web managers, and information on who participates in Web publishing. The agency's process for publishing content to the agency's public Web site includes five basic steps: (1) initial authorization of content, (2) screening content, (3) preparing content, (4) formatting content, and (5) publishing content. During the screening step, the content is checked for Web suitability and includes checks for copyright, OMB information collection requirements, persistent cookies, privacy, and sensitivity. The Web site includes numerous instructions and checklists for each step of the publishing process.

*6.h. Does the agency have a written policy or process for requiring machine-readability of public-facing agency Web sites (i.e., use of P3P[23])?*

MD and Handbook 3.14 discusses the use of P3P. The NRC public Web site contains a machine-readable P3P file that describes for the user's Web browser how NRC uses information collected through its online forms. It is the responsibility of the sponsor of each NRC subsite[24] outside of the NRC public Web site to ensure that their site complies with the OMB guidance on P3P.

### 3.7.2 Progress in Implementing OMB M-07-16

| OMB Requirement | OIG Response |
|---|---|
| *7. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."* | *Good* |

In response to the OMB memorandum M-07-16, NRC has accomplished the following:

- On September 19, 2007, NRC issued the *NRC Personally Identifiable Information Breach Policy* and the *NRC Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers*. NRC employees were notified of these policies via an agencywide announcement on that date. Carson Associates analyzed the breach notification policy and found it is compliant with the requirements outlined in OMB Memorandum M-07-16.
- A March 2008 memorandum to the agency from the CIO directed staff to review all administrative office files to reduce the unnecessary use of personally identifiable information (PII) and to report back to the privacy program officer that the review had been completed no later than May 30, 2008.
- In June 2008, the agency issued a revised computer security information protection policy in response to several OMB memoranda regarding the protection of agency sensitive information. The policy provided direction for protection of NRC information

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

[24] The term subsite is used to refer to a collection of Web pages within a larger site.

and information systems and will be included in the next revision of MD 12.5. The policy was provided to staff via an NRC Yellow Announcement.[25]

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

However, the agency has not fully implemented the provisions of OMB Memorandum M-07-16. NRC has completed all requirements except for the following:

- Agencies must review their current holdings of all PII and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete and reduce them to the minimum necessary for the proper performance of a documented agency function. Following the initial review, the agency must develop and make public a schedule by which they will periodically update the review of their holdings. NRC has not made a schedule public or determined the periodicity of a review of all holdings. However, the agency has implemented policy for the annual review of agency shared drives for PII.
- Agencies must encrypt all data on mobile computers/devices carrying agency data unless the data is determined not sensitive, in writing, by the agency's Deputy Secretary (or equivalent) or a senior-level official the Deputy Secretary may designate in writing. Only NIST-certified cryptographic modules may be used for encryption.[26] NRC has prohibited the removal of PII from agency controlled space, unless the mobile device is encrypted in accordance with NIST standards. Full implementation of the NRC enterprise encryption program is expected by June 30, 2010.
- Remote access should be allowed only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Currently, the agency requires a digital certificate and a user identifier and password for remote access. However, the certificate is not separate from the computer gaining access. Two-factor authentication has been incorporated into the encryption project that is expected to be completed by June 30, 2010.
- Agencies are required to ensure all individuals with authorized access to PII and their supervisors sign at least annually a document clearly describing their responsibilities. To ensure that all agency personnel are familiar with their responsibilities to protect sensitive information, including PII, NRC issues regular announcements to all employees. These announcements provide general guidance or address specific issues. Each notice directs agency personnel to an internal Privacy Act Web page, which provides staff access to

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

[26] See NIST's Website at http://csrc.nist.gov/cryptval/ for a discussion of the certified encryption products.

guidance, regulations, procedures, and training in the area of the Privacy Act. However, the agency is still developing a methodology for ensuring individuals with access to PII and their supervisors sign (at least annually) a document clearly describing their responsibilities.

## 3.8 Configuration Management (Question 8)

### *3.8.1 Configuration Policy and Common Security Configurations*

| OMB Requirement | OIG Response |
|---|---|
| *8.a. Is there an agencywide security configuration policy?* | *Yes* |
| *8.b. Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's Website at http://checklists.nist.gov.* | *Mostly (81-95% of the time)* |

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

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

The agency has also posted guidance on the NRC internal Web site requiring the use of hardening specifications for the different operating systems and software in use at the agency. Hardening specifications in use at the agency include benchmarks developed by the Center for Internet Security (CIS), the Defense Information Systems Agency (DISA) Gold Disk,[27] National Security Agency security configuration guides, and custom hardening specifications developed by the agency. The agency requires the use of the most recent version of the specified hardening specifications.

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

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

To determine the extent to which applicable systems apply common security configurations, Carson Associates reviewed the security test and evaluation results for the four systems selected for evaluation in FY 2008. The agency performs a vulnerability assessment during security control testing, which includes vulnerability scans, penetration tests, and hardening checks using the following tools:

- Nessus – A general-purpose scanning tool that provides information on network-based vulnerabilities.
- DISA Gold Disk – A Department of Defense tool that tests Windows-based hosts for compliance with the DISA Gold standard, including file and registry access control and auditing settings, running services, installed applications and patches, and user rights.
- CORE Impact – A specialized penetration testing tool that provides automated testing of known exploits against detected platforms, protocols, and services.
- CIS Benchmarks – NRC-approved security hardening specifications for a variety of platforms and software, prepared by CIS (http://www.cisecurity.org/).

The results from the vulnerability assessments for the four systems selected for evaluation in FY 2008 indicate that the systems apply common security configurations 81-95 percent of the time.

### 3.8.2 Federal Desktop Core Configuration (FDCC)

| OMB Requirement | OIG Response |
|---|---|
| *8.c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations.* | *Yes* |
| *8.c.2. New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology," is included in all contracts related to common security settings.* | *Yes* |
| *8.c.3. All Windows XP and Vista computing systems have implemented the FDCC security setting.* | *No* |

In March 2007, OMB issued a series of memoranda requiring agencies to develop plans for using Windows XP and Vista security configurations develop by NIST, the Department of Defense, and the Department of Homeland Security. Plans were to be submitted to OMB by May 1, 2007. The memoranda also require new acquisitions to include the configurations and require IT providers to certify their products operate effectively using the configurations. In June 2007, OMB issued a memorandum containing recommended language to use in solicitations to ensure new acquisitions include common configurations and IT providers certify their products operate effectively using the configurations. Agencies were required to report to OMB by February 1, 2008, the number of desktops using Windows XP and Vista and the number of those desktops that have implemented FDCC security settings. Agencies were also required to report to NIST the same information, as well as FDCC deviations for each operational environment/system role[28] present within the agency.

On April 27, 2007, the agency submitted its plan for using Windows XP and Vista security configurations to OMB. The agency's plan included all agency standard desktops/laptops.[29] On November 9, 2007, the agency issued a memorandum requiring a clause for ensuring new acquisitions include common security configurations in all new IT acquisition solicitations, contracts, agreements, purchase orders, delivery orders, and task orders awarded under the General Services Administration's Federal Supply Schedule. The memorandum also provided instructions for incorporating the clause into existing contracts, agreements, purchase orders, delivery orders, and task orders. On February 12, 2008, the agency submitted its FDCC status update to OMB and reported that the agency has a total of 4,856 managed desktops running Windows XP service pack 2, none of which are FDCC compliant. The report to OMB also included a breakdown of how many FDCC settings the agency does and does not meet. NIST has established two types of FDCC settings: group policy settings and application/registry settings. As of the February 2008 report to OMB, NRC met or exceeded 213 of the 237 group policy settings and met or exceeded 37 of the 62 application/registry settings that apply to the NRC environment. On March 31, 2008, the agency submitted its FDCC compliance report to NIST. When reporting to NIST, the agency reported only on the number of centrally-managed general-purpose desktops and reported a total of 27 deviations from the FDCC settings.

### FINDING C – Not All Windows XP and Vista Systems Have Implemented FDCC Security Settings (New Finding)

While the agency has adopted and implemented FDCC standard configurations, documented deviations, and included the new Federal Acquisition Regulation language in all contracts related to common security settings, Carson Associates found that not all Windows XP and Vista systems have implemented FDCC security settings. The agency's plan for using Windows XP and Vista security configurations included all agency standard desktops/laptops; however, the agency only reported to OMB and NIST on the number of centrally managed general purpose desktops connected to the NRC local area network. It is unclear whether the information reported to OMB and NIST also included centrally-managed general-purpose laptops, desktops and laptops that are not centrally managed, or desktops and laptops used as standalone[30] systems.

[28] NIST defines five operational environment/system roles for the purposes of FDCC reporting: centrally-managed general-purpose desktop, centrally-managed general-purpose laptop, development system, special use system, and other.

[29] Standard desktops and laptops only include those leased from a commercial vendor under the agency's seat management contract. They do not include desktops or laptops owned by the agency.

[30] Standalone refers to a desktop or laptop that is not configured for connectivity to the NRC local area network.

According to a 2005 OIG report on standalone PCs and laptops,[31] in 2005 there were approximately 117 standalone PCs and laptops that are used to process safeguards[32] and/or classified[33] information. However, the number of standalone PCs and laptops that do not process safeguards and/or classified information is unknown as these standalone PCs and laptops are not tracked in a central location. NRC has not included any standalone systems in its FDCC implementation plans or reports to OMB and NIST.

The 2005 OIG report found that security controls for standalone PCs and laptops were not adequate. The security controls were lacking because users were not given sufficient guidance on implementing security controls, the agency lacked a mechanism for assigning users responsibility for implementing security controls, and the agency lacked procedures for verifying that all required security controls were being implemented. This finding can be extended to include the lack of policies and procedures to implement the FDCC security settings. Many of the security controls the OIG found to be lacking are included in the FDCC security settings. Implementation of the FDCC security settings would correct many of the security controls found to be lacking in the OIG report.

## RECOMMENDATIONS

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

3. Develop agencywide policy and procedures regarding the implementation and monitoring of Federal Desktop Core Configuration controls for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless of whether or not they are connected to the agency's network.
4. Develop a process for verifying that all Federal Desktop Core Configuration controls are implemented for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless of whether or not they are connected to the agency's network.

[31] OIG-05-A-18, *System Evaluation of Security Controls for Standalone Personal Computers and Laptops*, September 22, 2005.

[32] Safeguards information is sensitive unclassified information that specifically identifies the (1) detailed security measures of a licensee or an applicant for the physical protection of special nuclear material or (2) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization facilities. Protection of this information is required pursuant to Section 147 of the Atomic Energy Act of 1954, as amended.

[33] Classified information is information (such as a document or correspondence) that is designated National Security Information, Restricted Data, or Formerly Restricted Data.

## 3.9 Incident Reporting (Question 9)

| OMB Requirement | OIG Response |
|---|---|
| *9.a. The agency follows documented policies and procedures for identifying and reporting incidents internally.* | *Yes* |
| *9.b. The agency follows documented policies and procedures for external reporting to US-CERT (http://www.us-cert.gov).* | *Yes* |
| *9.c. The agency follows documented policies and procedures for reporting to law enforcement.* | *Yes* |

On May 2, 2008, the agency issued a revised policy on computer security incident response and PII incident response. The policy provides direction for responding to computer security incidents affecting the NRC's systems, networks, and users, as well as PII incidents and will be included in the next revision of MD 12.5. The revised policy contains time frames for responding to such incidents, based on the criticality of the affected resources and the incident; formally establishes a Computer Security Incident Response Team (CSIRT) to respond to such incidents; and outlines the CSIRT's security incident response process. The CSIRT will include staff from the following offices: Computer Security Office, Office of Information Services, Office of Administration, and Office of Nuclear Security and Incident Response.

The agency has a page on its internal Web site with information on incident response, including what to do if a user discovers a virus; suspicious e-mail; or the deliberate or inadvertent release of sensitive, classified, or safeguards information. The agency has also developed incident response procedures for Exchange 2007/Outlook 2007 (electronic mail).

## 3.10 Security Awareness Training (Question 10)

| OMB Requirement | OIG Response |
|---|---|
| *10. Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?* | *Almost Always (96-100% of employees)* |

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

For FY 2008, all employees, including contractors, were required to take an online computer security awareness self-study course. All NRC employees and support contractors having network accounts were required to complete the course. Employees were also required to take and complete a quiz before receiving credit for taking the course. According to the agency, 97 percent of total employees (including contractors) have completed the online computer security awareness self-study course and completed the quiz. A score of 70 percent or higher is required to receive credit for completion of the course and quiz.

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

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

### FINDING D – Agency Still Developing Procedures for Ensuring Employees With Significant IT Security Responsibilities Receive Security Training (Repeat Finding)

While the agency meets the FISMA requirement to ensure all employees received IT security awareness training, the agency still has not met the requirement to provide specialized training for employees with significant security responsibilities as described in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*.

On April 3, 2008, the CISO issued a memorandum asking for support and action to ensure that all employees with significant IT security responsibilities are appropriately identified. The memorandum requires recipients of the memorandum to report back to the CISO by July 1, 2008, on the names of staff within their organization who have an IT security role as part of their official duties. The memorandum included a spreadsheet that can be used to identify the individuals with these roles and a template for completing the report. The information from the data call is currently being compiled into a database to develop a comprehensive role-based training plan. In March 2008, the agency contacted the Department of State to request training services under its Information Systems Security Line of Business, Information Assurance Role-Based Training Program. In addition to the role-based training the agency expects to be available via the Department of State, the agency provided a Defense in Depth – Securing Windows Server 2003 course to approximately 20 employees in January 2008 and provided role-based training for system owners in August 2008.

## 3.11 Collaborative Web Technologies and Peer-to-Peer File Sharing (Question 11)

| OMB Requirement | OIG Response |
|---|---|
| *11. Does the agency explain policies regarding the use of collaborative Web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agencywide training?* | *Yes* |

The IT Security Policies page on the agency's internal Web site specifically states that the installation of peer-to-peer (P2P) software on NRC computers is prohibited unless explicitly approved by the NRC Designated Approving Authority. The Web page also provides a link to P2P frequently asked questions. The FY 2008 online computer security awareness self-study course briefly discussed some types of collaborative Web technologies such as bulletin boards, discussion groups, instant messaging, and chat. The online computer security awareness self-study course also discussed the use of P2P and file-sharing software and reiterated the requirement to get explicit written approval from the NRC Designated Approving Authority prior to installing P2P software on NRC computers.

## 3.12 E-Authentication Risk Assessments (Question 12)

| OMB Requirement | OIG Response |
|---|---|
| *12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines?"* | *No* |
| *12.b. If the response is "No," then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.* | *See below.* |

In December 2003, OMB issued memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, which requires agencies to review new and existing electronic transactions to ensure the authentication processes provide the appropriate level of assurance. The FY 2008 FISMA guidance from OMB defines an e-authentication application as one that is Web-based, requires authentication, and extends beyond the borders of the agency's enterprise (e.g., multi-agency, governmentwide, or used by the public). Based on these criteria, NRC has determined that it does not have any e-authentication applications. Subsequent to the completion of fieldwork, the agency stated it has one e-authentication application in operation and another in development.

Carson Associates reviewed the e-authentication risk assessment and security plan for the agency's one operational e-authentication application and determined that the application has not operationally achieved the required assurance level in accordance with NIST SP 800-63, *Electronic Authentication Guidelines*.

[Page intentionally left blank]

# 4 Consolidated List of Recommendations

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

1. Update the NRC System Information Control Database to identify all interfaces between systems.
2. Develop and implement procedures to ensure interface information in the NRC System Information Control Database is consistent with interface information in security plans and risk assessments.
3. Develop agencywide policy and procedures regarding the implementation and monitoring of Federal Desktop Core Configuration controls for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless of whether or not they are connected to the agency's network.
4. Develop a process for verifying that all Federal Desktop Core Configuration controls are implemented for all desktop and laptop computers, including both those that are centrally managed under the agency's seat management contract and those that are owned by the agency regardless of whether or not they are connected to the agency's network.

[Page intentionally left blank]

# 5 Agency Comments

At an exit conference on September 16, 2008, agency officials agreed with the report's findings and recommendations and provided two editorial changes, which the OIG incorporated as appropriate. The agency opted not to submit formal comments.

[Page intentionally left blank]

## Appendix A. SCOPE AND METHODOLOGY

Carson Associates performed an independent evaluation of NRC's Implementation of FISMA for FY 2008. To conduct the independent evaluation, the team met with agency staff responsible for implementing the agency's information system security program, reviewed certification and accreditation documentation for the agency's operational information systems, and reviewed other documentation provided by the agency that demonstrated its implementation of FISMA.

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

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

This work was conducted between April 2008 and August 2008. Any information received from the agency subsequent to the completion of fieldwork was incorporated when possible. The work was conducted by Jane M. Laroussi, CISSP, and Joseph P. Rood, CISSP, CISA, from Richard S. Carson and Associates, Inc.

[Page intentionally left blank]

# Appendix B. FY 2008 OMB FISMA REPORTING TEMPLATE FOR IGs

This appendix contains the FY 2008 OMB FISMA Reporting Template for IGs (referred to by OMB as Section C) that will be included in the agency's FISMA submission to OMB.

## Section C - Inspector General: Questions 1 and 2

**Agency Name:** **Nuclear Regulatory Commission** **Submission date:** **September 19, 2008**

### Question 1: FISMA Systems Inventory

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

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

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

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

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

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

| | | Question 1 | | | | | | Question 2 | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | a.<br>Agency Systems | | b.<br>Contractor Systems | | c.<br>Total Number of Systems (Agency and Contractor systems) | | a.<br>Number of systems certified and accredited | | b.<br>Number of systems for which security controls have been tested and reviewed in the past year | | c.<br>Number of systems for which contingency plans have been tested in accordance with policy | |
| **Bureau Name** | **FIPS 199 System Impact Level** | Number | Number Reviewed | Number | Number Reviewed | Total Number | Total Number Reviewed | Total Number | Percent of Total | Total Number | Percent of Total | Total Number | Percent of Total |
| | High | 11 | 1 | 1 | 0 | 12 | 1 | 1 | 100% | 1 | 100% | 1 | 100% |
| | Moderate | 17 | 2 | 9 | 0 | 26 | 2 | 2 | 100% | 2 | 100% | 2 | 100% |
| | Low | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 100% | 1 | 100% | 1 | 100% |
| | Not Categorized | 0 | 0 | 0 | 0 | 0 | 0 | | | | | | |
| | **Sub-total** | **28** | **3** | **11** | **1** | **39** | **4** | **4** | 100% | **4** | 100% | **4** | 100% |
| **Component/Bureau** | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | | **0** | | **0** | |
| **Component/Bureau** | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | | **0** | | **0** | |
| **Component/Bureau** | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | | **0** | | **0** | |
| **Component/Bureau** | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | | **0** | | **0** | |
| **Component/Bureau** | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | | **0** | | **0** | |
| **Agency Totals** | **High** | **11** | **1** | **1** | **0** | **12** | **1** | **1** | 100% | **1** | 100% | **1** | 100% |
| | **Moderate** | **17** | **2** | **9** | **0** | **26** | **2** | **2** | 100% | **2** | 100% | **2** | 100% |
| | **Low** | **0** | **0** | **1** | **1** | **1** | **1** | **1** | 100% | **1** | 100% | **1** | 100% |
| | **Not Categorized** | **0** | **0** | **0** | **0** | **0** | **0** | **0** | | **0** | | **0** | |
| | **Total** | **28** | **3** | **11** | **1** | **39** | **4** | **4** | 100% | **4** | 100% | **4** | 100% |

## Section C - Inspector General: Question 3

| | | |
|---|---|---|
| Agency Name: | Nuclear Regulatory Commission | |
| Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory | | |
| 3.a. | **The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.**<br>Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.<br>Response Categories:<br>- Rarely- for example, approximately 0-50% of the time<br>- Sometimes- for example, approximately 51-70% of the time<br>- Frequently- for example, approximately 71-80% of the time<br>- Mostly- for example, approximately 81-95% of the time<br>- Almost Always- for example, approximately 96-100% of the time | Almost Always (96-100% of the time) |
| 3.b. | **The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.**<br>Response Categories:<br>- The inventory is approximately 0-50% complete<br>- The inventory is approximately 51-70% complete<br>- The inventory is approximately 71-80% complete<br>- The inventory is approximately 81-95% complete<br>- The inventory is approximately 96-100% complete | Inventory is 96-100% complete |
| 3.c. | **The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.** | Yes |
| 3.d. | **The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.** | Yes |
| 3.e. | **The agency inventory is maintained and updated at least annually. Yes or No.** | Yes |
| 3.f. | **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.** | |

| Component/Bureau | System Name | Exhibit 53 Unique Project Identifier (UPI) {must be 23-digits} | Agency or Contractor system? |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Section C - Inspector General: Questions 4 and 5

| | |
|---|---|
| Agency Name: | **Nuclear Regulatory Commission** |

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

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

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

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

| | | |
|---|---|---|
| **4.a.** | The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency. | Almost Always (96-100% of the time) |
| **4.b.** | When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s). | Almost Always (96-100% of the time) |
| **4.c.** | Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly). | Almost Always (96-100% of the time) |
| **4.d.** | Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis. | Almost Always (96-100% of the time) |
| **4.e.** | IG findings are incorporated into the POA&M process. | Almost Always (96-100% of the time) |
| **4.f.** | POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources. | Almost Always (96-100% of the time) |
| **POA&M process comments:** | NRC has two primary tools for tracking IT security weaknesses. At a high level, NRC uses the POA&Ms required by OMB to track (1) corrective actions from the OIG annual independent evaluation, (2) corrective actions from the agency's annual review, and (3) recurring FISMA and IT security action items such as annual security control assessments and annual contingency plan testing. The POA&Ms may also include corrective actions resulting from other security studies conducted by or on behalf of NRC. The more specific corrective actions associated with the certification and accreditation process (e.g., corrective actions resulting from risk assessments and security control testing) are tracked in Rational ClearQuest as change requests using the project management methodology process for change management. | |

### Question 5: IG Assessment of the Certification and Accreditation Process

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

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

| | | |
|---|---|---|
| **5.a.** | **The IG rates the overall quality of the Agency's certification and accreditation process as:**<br>Response Categories:<br>- Excellent<br>- Good<br>- Satisfactory<br>- Poor<br>- Failing | Satisfactory |

| | | | |
|---|---|---|---|
| **5.b.** | **The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply) | Security plan | X |
| | | System impact level | X |
| | | System test and evaluation | X |
| | | Security control testing | X |
| | | Incident handling | |
| | | Security awareness training | |
| | | Configurations/patching | X |
| | | Other: | Risk assessment |
| **C&A process comments:** | Incident handling and security awareness training were evaluated at the agency level. | | |

| | | |
|---|---|---|
| **Section C - Inspector General: Questions 6, 7, and 8** | | |
| **Agency Name:** | **Nuclear Regulatory Commission** | |
| **Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process** | | |
| **6** | **Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.**<br>Response Categories:<br>- Response Categories:<br>- Excellent<br>- Good<br>- Satisfactory<br>- Poor<br>- Failing | Excellent |
| **Comments:** | | |
| **7** | **Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.**<br>Response Categories:<br>- Response Categories:<br>- Excellent<br>- Good<br>- Satisfactory<br>- Poor<br>- Failing | **Good** |
| **Comments:** | | |
| **Question 8: Configuration Management** | | |
| **8.a.** | **Is there an agency-wide security configuration policy? Yes or No.** | Yes |
| **Comments:** | | |
| **8.b.** | **Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.**<br>**Response categories:** | Mostly (81-95% of the time) |
| | - Rarely- for example, approximately 0-50% of the time<br>- Sometimes- for example, approximately 51-70% of the time<br>- Frequently- for example, approximately 71-80% of the time<br>- Mostly- for example, approximately 81-95% of the time<br>- Almost Always- for example, approximately 96-100% of the time | |
| **8.c.** | **Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:** | |
| | **c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.** | Yes |
| | **c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.** | Yes |
| | **c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.** | No |

## Section C - Inspector General: Questions 9, 10 and 11

| | | |
|---|---|---|
| Agency Name: | Nuclear Regulatory Commission | |
| | Question 9: Incident Reporting | |
| Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement.<br>If appropriate or necessary, include comments in the area provided below. | | |
| 9.a. | The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No. | Yes |
| 9.b. | The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov) | Yes |
| 9.c. | The agency follows documented policies and procedures for reporting to law enforcement. Yes or No. | Yes |
| Comments: | | |
| | Question 10: Security Awareness Training | |
| Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities?<br>Response Categories:<br>- Rarely- or approximately 0-50% of employees<br>- Sometimes- or approximately 51-70% of employees<br>- Frequently- or approximately 71-80% of employees<br>- Mostly- or approximately 81-95% of employees<br>- Almost Always- or approximately 96-100% of employees | | Almost Always (96-100% of employees) |
| | Question 11: Collaborative Web Technologies and Peer-to-Peer File Sharing | |
| Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No. | | **Yes** |
| | Question 12: E-Authentication Risk Assessments | |
| 12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, "Electronic Authentication Guidelines"? Yes or No. | | **No** |
| 12.b. If the response is "No", then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation. | | The agency's one operational e-authentication application has not operationally achieved the required assurance level in accordance with NIST SP 800-63, *Electronic Authentication Guidelines*. |