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

Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act (FISMA) for Fiscal Year 2004

OIG–04-A-22 September 30, 2004

EVALUATION REPORT

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

September 30, 2004

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: INDEPENDENT EVALUATION OF NRC'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) FOR FISCAL YEAR 2004 (OIG-04-A-22)

This evaluation report titled*, Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act for Fiscal Year 2004.* Appendix B contains the OIG 2004 Federal Information Security Management Act Report template to the Office of Management and Budget. This report reflects the results of the independent evaluation performed by Richard S. Carson & Associates, Inc. on behalf of the NRC Office of the Inspector General.

Based on its review, Richard S. Carson & Associates, Inc., determined that the NRC's information security program has the following weaknesses:

- NRC Management Directive 12.5, *NRC Automated Information Security Program*, contains sensitive information that is publicly available.
- Several required security documents need updating.
- Some security processes need further improvement.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on September 22, 2004, NRC officials provided comments concerning the draft audit report and opted not to submit formal written comments to this report.

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

Attachment: As stated

Distribution List

B. John Garrick, Chairman, Advisory Committee on Nuclear Waste
Mario V. Bonaca, Chairman, Advisory Committee on Reactor Safeguards
John T. Larkins, Executive Director, Advisory Committee on Reactor Safeguards/Advisory Committee on Nuclear Waste
G. Paul Bollwerk, III, Chief Administrative Judge, Atomic Safety and Licensing Board Panel
Karen D. Cyr, General Counsel
John F. Cordes, Jr., Director, Office of Commission Appellate Adjudication
Jesse L. Funches, Chief Financial Officer
Janice Dunn Lee, Director, Office of International Programs
William N. Outlaw, Director of Communications
Dennis K. Rathbun, Director, Office of Congressional Affairs
Eliot B. Brenner, Director, Office of Public Affairs
Annette Vietti-Cook, Secretary of the Commission
Patricia G. Norry, Deputy Executive Director for Management Services, OEDO
William F. Kane, Deputy Executive Director for Homeland Protection and Preparedness, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research and State Programs, OEDO
Ellis W. Merschoff, Deputy Executive Director for Reactor Programs, OEDO
William M. Dean, Assistant for Operations, OEDO
Jacqueline E. Silber, Chief Information Officer
Michael L. Springer, Director, Office of Administration
Frank J. Congel, Director, Office of Enforcement
Guy P. Caputo, Director, Office of Investigations
Paul E. Bird, Director, Office of Human Resources
Corenthis B. Kelley, Director, Office of Small Business and Civil Rights
Jack R. Strosnider, Director, Office of Nuclear Material Safety and Safeguards
James E. Dyer, Director, Office of Nuclear Reactor Regulation
Carl J. Paperiello, Director, Office of Nuclear Regulatory Research
Paul H. Lohaus, Director, Office of State and Tribal Programs
Roy P. Zimmerman, Director, Office of Nuclear Security and Incident Response
Samuel J. Collins, Regional Administrator, Region I
William D. Travers, Regional Administrator, Region II
James L. Caldwell, Regional Administrator, Region III
Bruce S. Mallett, Regional Administrator, Region IV
Office of Public Affairs, Region I
Office of Public Affairs, Region II
Office of Public Affairs, Region IV

"Independent Evaluation of NRC's Implementation of the Federal Information Security Management Act For Fiscal Year 2004"

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

September 24, 2004

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

Richard S. Carson & Associates, Inc., on behalf of the Office of the Inspector General of the U.S. Nuclear Regulatory Commission (NRC), completed this Independent Evaluation Report, and the NRC 2004 Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) Report, which is included as Appendix B. The Independent Evaluation Report identifies specific findings and recommendations for resolution of identified weaknesses.

PURPOSE

The objectives of the independent evaluation of NRC's information security program were to:

1. Test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; and
2. Assess compliance with the Federal Information Security Management Act and related information security policies, procedures, standards, and guidelines.

RESULTS IN BRIEF

Over the past year, NRC continued to improve its security program. For example, NRC:

- Completed a majority of program and system level corrective actions identified in the FY 2003 FISMA review, including additional corrective actions identified throughout FY 2004 (approximately 83%).
- Completed a risk assessment, security plan, business continuity plan, and certified and accredited one of the new major applications under development.
- Completed annual business continuity plan testing for sixteen of the seventeen major applications and general support systems at NRC.
- Developed a process for updating the NRC system inventory on a semi-annual basis.
- Developed procedures for implementing security configurations on NRC servers.

However, the independent evaluation identified the following information security program weaknesses. None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in OMB guidance.

- NRC Management Directive 12.5, *NRC Automated Information Security Program*, contains sensitive information, but it was publicly available.

- Agreements with the two Federal agencies providing services to NRC need updating.
- Four system certifications and accreditations need updating.
- One risk assessment needs updating.
- One system business continuity plan needs updating.
- NRC's corrective action tracking process needs further improvement.
- The agency's plan of action and milestones needs improvement.
- The agency's certification and accreditation process needs improvement. Specifically, the agency needs to develop processes for (1) ensuring security documentation supporting system certification and accreditation is consistent with National Institute of Standards and Technology guidelines, (2) ensuring security protection requirements (confidentiality, integrity, availability) are consistently defined in security plans and self-assessments, and (3) ensuring security test and evaluation in support of certification and accreditation is comprehensive and independent.

RECOMMENDATIONS

This report makes sixteen recommendations to the Executive Director for Operations. A consolidated list of recommendations can be found on page 31 of this report.

AGENCY COMMENTS

On September 22, 2004, the Executive Director for Operations provided comments concerning the draft Independent Evaluation Report and NRC 2004 OMB FISMA Report. We modified the reports as we determined appropriate in response to these comments.

ABBREVIATIONS AND ACRONYMS

ADAMS	Agencywide Document Access and Management System
BCP	Business Continuity Plan
C&A	Certification and Accreditation
CFR	Code of Federal Regulations
CIO	Chief Information Officer
DDMS	Digital Data Management System
DOI	Department of the Interior
FFS	Federal Financial System
FISMA	Federal Information Security Management Act
FPPS	Federal Personnel and Payroll System
FY	Fiscal Year
IPSS	Integrated Personnel Security System
ISSO	Information System Security Officer
IT	Information Technology
ITSSTS	Information Technology Systems Security Tracking System
LAN/WAN	Local Area Network/Wide Area Network
MD	Management Directive
NBC	National Business Center
NIH	National Institutes of Health
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
SITSO	Senior Information Technology Security Officer
SP	Special Publication
US-CERT	United States Computer Emergency Readiness Team

[Page intentionally left blank]

TABLE OF CONTENTS

Appendices

[Page intentionally left blank]

1 Background

Richard S. Carson & Associates, Inc. (Carson Associates), on behalf of the Office of the Inspector General (OIG) of the U.S. Nuclear Regulatory Commission (NRC), completed this Independent Evaluation Report, and the NRC 2004 Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) Report, which is included as Appendix B. The Independent Evaluation Report identifies specific findings and recommendations for resolution of identified weaknesses.

On December 17, 2002, the President signed the E-Government Act of 2002 (Public Law 107-347), which includes the Federal Information Security Management Act of 2002[1]. FISMA outlines the information security management requirements for agencies, which include an annual review by the agency, an independent evaluation of an agency's information security program and practices by the agency's inspectors general, and an evaluation of the effectiveness of information security control techniques. FISMA also requires an assessment of compliance with requirements and related information security policies, procedures, standards, and guidelines. The annual agency reviews and the OIG independent evaluations are intended to provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

The independent evaluation comprises four elements — evaluation of the implementation of NRC's information security program, evaluation of progress towards completing corrective actions addressed within the FY 2003 Plan of Action and Milestones (POA&M), review of the system self-assessments prepared by NRC, and verification and testing of information security controls for six representative information systems. Four of the systems are NRC systems, and two of the systems are systems used by NRC, but owned by another Federal agency. The results of the independent evaluation are presented in this Independent Evaluation Report, which presents recommendations to address the weaknesses identified during the evaluation.

2 Purpose

The objectives of the independent evaluation of NRC's information security program were to:

1. Test the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems; and
2. Assess compliance with FISMA and related information security policies, procedures, standards, and guidelines.

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

3 Findings

Over the past year, NRC continued to improve its security program. For example, NRC:

- Completed a majority of program and system level corrective actions identified in the FY 2003 FISMA review, including additional corrective actions identified throughout FY 2004 (approximately 83%).
- Completed a risk assessment, security plan, business continuity plan, and certified and accredited one of the new major applications under development.
- Completed annual business continuity plan testing for sixteen of the seventeen major applications and general support systems at NRC.
- Developed a process for updating the NRC system inventory on a semi-annual basis.
- Developed procedures for implementing security configurations on NRC servers.

However, the independent evaluation identified the following information security program weaknesses. None of these weaknesses are considered to be significant deficiencies[2] or reportable conditions[3] as defined in OMB guidance.

- NRC Management Directive 12.5, *NRC Automated Information Security Program*, contains sensitive information, but it was publicly available.
- Agreements with the two Federal agencies providing services to NRC need updating.
- Four system certifications and accreditations need updating.
- One risk assessment needs updating.
- One system business continuity plan needs updating.
- NRC's corrective action tracking process needs further improvement.
- The agency's POA&M needs improvement.
- The agency's certification and accreditation process needs improvement. Specifically, the agency needs to develop processes for (1) ensuring security documentation supporting system certification and accreditation is consistent with National Institute of Standards and Technology (NIST) guidelines, (2) ensuring security protection requirements (confidentiality, integrity, availability) are consistently defined in security plans and self-assessments, and (3) ensuring security test and evaluation in support of certification and accreditation is comprehensive and independent.

[2] A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

[3] A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management and/or external agencies.

The following sections present the detailed findings from the independent evaluation. The format of the following sections is based on the sections of the NRC 2004 OMB FISMA Report, which can be found in Appendix B.

3.1 System Inventory and Information Technology Security Performance

NRC 2004 OMB FISMA Report Section A

3.1.1 NRC Programs and Systems

NRC 2004 OMB FISMA Report A.1.a, A.1.b, A.3.f

NRC Programs

Carson Associates reviewed NRC's one program. NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, defines NRC's automated information systems security program. MD 12.5 was updated in September 2003 to include the following updates:

- New security policies and procedures developed since MD 12.5 was last updated were incorporated. These policies include, but are not limited to Guidelines for the Use of Password Checking Software, Incident Response Procedures, Operating and System Software Maintenance Procedures, and NRC's Firewall Policy.
- The system identification diagram that was used to categorize NRC information systems was removed and replaced with a full description of each system category (major application, general support system, listed, and other). MD 12.5 also includes a new table, "Security Planning and Reporting Requirements by System Type."
- Additional text was added to clarify who is responsible for developing and maintaining the system inventory. It states that Regional Administrators and Office Directors are to provide input into the system inventory, and the system sponsors/owners are responsible for ensuring that all office-sponsored systems are properly categorized and accurately reflected in the master inventory of systems maintained by the Office of the Chief Information Officer (OCIO). Each office will work with OCIO to update and revalidate the master inventory of systems on an annual basis.

The various policies included in MD 12.5 can be found on the NRC Customer Service Branch website, and the on-line versions are up-to-date. OCIO also provides supplemental information security guidance on the NRC internal web site, including:

- NRC Password and Warning Banner Guidance
- Guidelines for Modem Usage
- Processing and Handling Safeguards Information in the NRC Unclassified Local Area/Wide Area Network Environment
- Templates for risk assessments, security plans, and security test and evaluation plans.

MD 12.5 Contains Sensitive Information, But It Was Publicly Available

During the FY 2004 FISMA review, Carson Associates discovered that MD 12.5 was available on the NRC public web site. In the past, this directive was only available on the NRC internal web site. According to NRC policy and regulations, the NRC Management Directive System has always been available to the public either on CD-ROM, or in the Commission's Public Document Room. However, publication of the Management Directives on the NRC public web site provides a much larger population, both in the United States and internationally, access to the documents.

MD 12.5 contains sensitive information that should not be disclosed to the public. For example, MD 12.5 includes the NRC firewall policy, with a note that the current firewall policy can be found on the NRC internal web site. However, the agency has determined that this policy is too sensitive to be posted even on the NRC internal web site, and it can only be obtained by requesting it from OCIO.

NRC has removed MD 12.5 from the NRC public web site and from the Agencywide Document Access and Management System (ADAMS). However, Carson Associates found at least one document in ADAMS with MD 12.5 attached, and the public can still access MD 12.5 in the NRC Public Document Room.

RECOMMENDATION

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

1. Remove sensitive data from Management Directive 12.5, *NRC Automated Information Security Program*, which should not be disclosed to the public.

NRC Systems

NRC has a total of seventeen production systems – thirteen are major applications and four are general support systems. NRC also has two systems currently in development. Carson Associates reviewed four of the seventeen production systems. The system evaluation objectives were to review and evaluate the security controls for the systems. The systems were evaluated by reviewing system documentation maintained by OCIO. As recommended by OMB, Carson Associates reviewed the following types of documents for adherence to standards and consistency with guidelines issued by NIST.

- Risk Assessment
- Security Plan
- Business Continuity Plan
- Security Test and Evaluation Plan and Report
- Certification and Accreditation Report
- Privacy Impact Assessment
- Draft FY 2004 Self-Assessment

The documents were reviewed to determine whether they are consistent with NIST guidance and whether they describe the security controls in place for the systems. Carson Associates found that in some cases (1) security documentation is not consistent with NIST guidelines, (2) security protection requirements are inconsistent within system security documentation, and (3) findings and recommendations resulting from testing system security controls are not consistently being tracked. Separate system evaluation reports were prepared and delivered to the agency. The overall findings from the system evaluations are discussed further in *Section 3.2, Assessment of the POA&M Process*, and *Section 3.3, Assessment of the Certification and Accreditation Process*.

3.1.2 Contractor Operations or Facilities

NRC 2004 OMB FISMA Report A.1.c, A.3.a, A.3.b, A.3.c, A.3.f

NRC uses NIST Special Publication (SP) 800-26, *Self-Assessment Guide for Information Technology Systems,* for reviewing their own programs and systems. However, NRC primarily uses methods other than NIST SP 800-26 for reviewing contractor operations and facilities. NRC has a total of seven contractor operations or facilities, and Carson Associates reviewed three of them. NRC presumes that the two agencies supporting NRC are also following FISMA and NIST guidelines (these agencies have not allowed NRC to conduct their own review). Carson Associates verified that there are agreements in place with the two Federal agencies providing services to NRC. Carson Associates also reviewed a recent security review for one contractor facility.

For two contractors who provide support to NRC, and one contractor who maintains one of NRC's major applications, management officials stated that these contractors, who have access to NRC information technology (IT) resources, must have security guidelines written into their contracts, must follow NRC security procedures, and new contracts must specify use of NIST guidance for security. Carson Associates could not determine how NRC ensures operations or facilities at one location are adequately secure and meet Federal policy and guidelines.

Carson Associates also met with OCIO staff to discuss any other methods NRC uses to ensure contractor operations or facilities are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. OCIO staff stated that for two of the contractors, they are treated just like one of the NRC's regional offices – they are considered trusted foreign networks. There is security language in the contracts currently in place with the two contractors, and NRC has day-to-day relationships with both companies.

Agreements with the Two Federal Agencies Providing Services to NRC Need Updating

Carson Associates reviewed services provided to NRC by the Department of the Interior (DOI), and the National Institutes of Health (NIH). NRC uses two systems hosted and supported by DOI – the Federal Financial System (FFS) and the Federal Personnel and Payroll System (FPPS). NIH provides NRC with Internet connectivity, and two applications that are part of the Fee Systems are housed on a mainframe located at NIH. The objective of the reviews was to determine whether the services and facilities provided by DOI and NIH are adequately secure

and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

Department of the Interior

For FFS and FPPS, Carson Associates attempted to get up-to-date security documentation for the two systems in order to review the security controls in place for the systems. For most of the month of July 2004, Carson Associates was in contact with several DOI staff members in both the National Business Center[4] (NBC) and the DOI OIG. Carson Associates was in possession of some documents for both systems, but needed to know if the documents were up-to-date, and needed other documents necessary to conduct a system review. Most of the documents were from an interim accreditation that was granted in FY 2003. Both systems were fully accredited in FY 2004, so the intent was to obtain the documentation supporting the full accreditation.

Carson Associates and the NRC OIG had a conference call with the DOI OIG to discuss a current FISMA study being conducted by the DOI OIG on their information systems, including FFS and FPPS. They described what they were doing for the study and discussed some of the issues that had been found so far. They decided to do the study because of the large number of requests from agencies using NBC services for information on their security controls and practices. They will do this review every year, and for future years the reports are planned to be ready by the end of July (so agencies can use them for their FISMA reviews).

The DOI review found that NBC's information security management program and practices met FISMA requirements with a few minor exceptions. The DOI Evaluation Report, "Review of Information System Security over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of the Interior Clients," stated that overall agreements between NBC and their clients are supposed to include three separate agreements.

- Service Level Agreements – defines specific tasks to be performed and roles and responsibilities of the respective parties.
- Security Service Agreements – defines security roles and responsibilities of the respective parties.
- Interconnect Security Agreements – defines the roles and responsibilities for client network management in connecting to NBC systems and applications.

The DOI OIG review found that of the fifteen agreements reviewed, only one had a Security Service Agreement, and none had Interconnect Security Agreements. Carson Associates was provided a Security Services Agreement between NBC and NRC. Carson Associates was not provided with a Service Level Agreement or an Interconnect Security Agreement between NBC and NRC.

[4] The DOI National Business Center serves as the systems manager and general purpose computing host for systems supporting budget, procurement and contracts, personnel management, financial and accounting, E-government, and other general administrative systems.

The DOI report also stated that to ensure that risks are understood and security protections are established to reduce the risks to acceptable levels, DOI believes that an exchange of system security plans between NBC and its clients should be accomplished. This exchange will provide each party the necessary information to understand the level of importance each party assigns to the sensitivity and criticality of the systems and information as well as describing the respective control environments. Through these exchanges NBC will have a better understanding of the risks to its systems and external clients' requirements to ensure that appropriate protections are implemented.

The Security Services Agreement between NBC and the NRC does state that the NBC will provide copies of certification and accreditation documents to clients on request, however, it does not specifically mention security plans as a type of document that NBC will provide. Carson Associates also found a few places in the Security Services Agreement where information is not accurate or up-to-date. A link to an NBC web page on page three does not work, and the NRC contact information on page ten needs to be updated.

RECOMMENDATIONS

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

2. Update the Security Services Agreement between the Department of the Interior National Business Center and NRC to include a requirement to exchange relevant system security plans.

3. Develop a Service Level Agreement and Interconnect Security Agreement between the Department of the Interior National Business Center and NRC as described in the DOI Evaluation Report, "Review of Information System Security over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of the Interior Clients."

National Institutes of Health

Two of the Fee Systems applications reside on a mainframe housed in the NIH Data Center. Carson Associates reviewed certification and accreditation documentation for the NIH Data Center as part of the overall system review of the Fee Systems. The documentation was reviewed in order to determine whether agency program officials and the agency Chief Information Officer (CIO) have used appropriate methods to ensure that services provided by NIH for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. NIH also provides NRC with Internet connectivity.

NRC developed a Memorandum of Understanding between NRC and NIH, dated January 2003. It is a one page document describing the services NIH provides to NRC and states that all parties agree to ensure compliance with applicable Federal and respective agency automated information systems security policies, mandates and instructions that will ensure the continued confidentiality, integrity, and availability of information being processed by or through this

system. The Memorandum of Understanding is to be reviewed annually and will remain in effect until terminated in writing.

NIH and NRC also developed a Joint Network Interconnection Security Agreement, dated December 2003. This is a more comprehensive agreement between the two agencies and outlines system security considerations for both agencies. The document includes sections describing the purpose, authority, and interconnection statement of requirements. The document also includes a section describing system security considerations, including services offered, data sensitivity, user community, information exchange security, communication/IT security points of contact, responsible parties, trusted behavior expectations, formal security policy, and incident reporting. The document outlines NIH and NRC responsibilities regarding physical security, identification and authentication, anti-virus software, system configuration, warning banners, remote access, wireless security, and encryption. It concludes with a discussion of network management, compliance, and confidentiality.

The Network Interconnection Security Agreement states that a Service Level Agreement signed by NIH and NRC governs certain services provided by NIH for a fee. NRC provided a copy of a Service Level Agreement between NIH and NRC that was signed by NRC at the end of March 2003, and by NIH at the beginning of April 2003. The agreement became effective April 1, 2003, and remained in effect until September 30, 2003. The agreement describes the services provided by NIH to NRC, including network support and maintenance services. The agreement discusses services not supported, customer responsibilities, and costs to NRC. Appendices to the agreement include an NRC contact list, billing information, escalation procedures, and NRC points of contact for problem resolution. The agency provided a copy of a draft of the agreement that would replace the agreement that expires September 30, 2003, but was not able to provide a final, signed agreement.

RECOMMENDATION

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

4. Update the Service Level Agreement between NRC and the National Institutes of Health.

3.1.3 Certification and Accreditation

NRC 2004 OMB FISMA Report A.2.a

Fourteen of the seventeen systems have full accreditation, and three have interim accreditations. The interim accreditation for one system expired in July 2004. One system was granted an extension to the interim accreditation and it will expire at the end of September 2004. Full accreditation of these two systems was scheduled for 4th Quarter FY 2004, and there are POA&M items for tracking the accreditations, however the accreditations have not been completed as of September 15, 2004. Full accreditation for the third system with interim accreditation is scheduled for the 1st Quarter FY 2005.

Four Certification and Accreditations are Not Up-To-Date

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, states that security certification directly supports security accreditation by providing authorizing officials with important information necessary to make credible, risk-based decisions on whether to place information systems into operation or continue their current operation. This information is produced by assessing the security controls in the information system 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.

While none of the seventeen systems have signed certification and accreditation (C&A) memoranda that are more than three years old, five of the seventeen systems have C&A reports that are more than three years old. The C&A reports are the documents that provided the authorizing officials with the information necessary to accredit the systems. Accreditation memoranda for the five systems with outdated C&A reports were not signed until almost a year (or more) had past since the C&A testing was conducted. Re- accreditation of one of the five systems with an outdated C&A report was scheduled for 4th Quarter FY 2004, and there is a POA&M item for tracking the re-accreditation, however the re-accreditation had not been completed as of September 15, 2004. Re-accreditation of the remaining four systems is scheduled for FY 2005.

RECOMMENDATIONS

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

5. Re-certify and re-accredit the NRC Data Center/Telecommunications System.

6. Re-certify and re-accredit the NRC Local Area Network/Wide Area Network.

7. Re-certify and re-accredit the Emergency Response Data System.

8. Re-certify and re-accredit the Emergency Telecommunications System.

One Risk Assessment is Not Up-To-Date

All seventeen systems have risk assessments. Five of the systems' risk assessments should have been updated this fiscal year, as they were more than three years old. Four of the outdated risk assessments were updated in FY 2004, and the review team verified and validated the updates. The risk assessment for the NRC local area network/wide area network (LAN/WAN) has not been updated since February 2001. However, separate updates to the risk assessment were developed as LAN/WAN subsystems were certified and accredited. One of the systems in development, the Digital Data Management System (DDMS), also has a risk assessment.

RECOMMENDATION

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

9. Update the NRC Local Area Network/Wide Area Network Risk Assessment.

All Security Plans are Up-To-Date

Sixteen of the seventeen systems have security plans. The security plan for the seventeenth system is scheduled for completion by the end of September 2004. Four of the systems' security plans should have been updated this fiscal year, as they were more than three years old. All four of the outdated security plans were updated in FY 2004, and the review team verified and validated the updates. One of the systems in development, DDMS, also has a security plan.

MD 12.5 also requires security plans for "listed" systems, and systems that process classified and unclassified safeguards information. A "listed" system is a computerized information system or application that processes sensitive information requiring additional security protections, and that may be important to the operations of an NRC office or region, but is not a major application when viewed from an agency perspective. For example, some NRC offices have developed a number of additional non-major applications that are processing sensitive information such as Privacy Act information, or sensitive contractual and financial information.

As a result of a POA&M item from the agency's own FY 2003 FISMA review, the agency issued a memorandum in February 2004 instructing Office Directors and Regional Administrators to ensure that information systems sponsored by their office that process or store classified information, safeguards information, or sensitive information have individual security plans. The memorandum included instructions for preparing the security plans, as well as a template, as attachments. Carson Associates obtained a report from the agency's internal tracking system, the Information Technology Systems Security Tracking System (ITSSTS), of all "listed" systems at NRC and the status of their security plans. Carson Associates selected seventeen "listed" systems to check for the existence of security plans. Security plans for thirteen of the seventeen systems were located in files maintained by OCIO. Security plans for four of the systems were not on file with OCIO. Security plans for these systems have either been requested, or sent back for revisions, and their current status is reflected in the ITSSTS report.

3.1.4 Security Control Costs and Information Technology Investments

NRC 2004 OMB FISMA Report A.2.b, A.3.g

NRC has developed several policies and procedures to ensure that security control costs are integrated into the life cycle of NRC systems. These include MD 12.5, MD 2.2, *Capital Planning and Investment Control*, and MD 2.5, *System Development Life Cycle Management Methodology*.

The Exhibit 53 submitted to OMB in 2004 for budget year 2005 reflects that IT security costs are included in the investments for all NRC major applications and general support systems with the

exception of two systems. The agency stated that these two systems had less than one half of one percent in security costs; therefore per OMB guidance they were rounded to zero. All system levels POA&Ms submitted by the agency at the end of the 4th Quarter FY 2004 have unique project identifiers that match those used on the Exhibit 53, and include total security costs for completing the corrective actions.

A major IT investment (Tier 1) meets or exceeds a control phase cost threshold of $1,500,000 (or $500,000 for financial management systems), or has other characteristics that are of particular interest to NRC management or to the OMB. A Tier 2 investment is one that meets or exceeds a control phase cost threshold of $500,000 (but below the Tier 1 $1,500,000 threshold), or requires some level of management control and oversight to effectively deal with special security, architecture, coordination, staffing, or other concerns presented by these investments. A Tier 3 investment is one that does not exceed a control phase cost threshold of $500,000 and has no other special characteristics that would classify it as Tier 1 or Tier 2.

Office Directors and Regional Administrators must submit information on office or regional IT investments, needs, and plans to the CIO in accordance with NRC's capital planning and investment control process, or as requested, to support agencywide IT planning, budgeting, or investment control.

The CIO is responsible for the following related to approval of major IT investments:

- Reviewing and approving security certifications and accreditations for NRC information systems, including risk analysis results, security plans, contingency plans, and security-related elements of investment justifications submitted in accordance with NRC capital planning and investment control.
- Developing and implementing agencywide IT planning, budgeting, and investment control policies, processes, and procedures that support NRC's mission and meet the requirements of Federal statutes and regulations and are consistent with NRC's overall planning, budgeting, and performance management process.
- Reviewing and approving business cases for all IT investments during the selection phase, and for referring Tier 1 IT investments to the Executive Director for Operations for review and approval.
- Ensuring that proposed new IT investments are not duplicative of other planned or ongoing projects or application systems, unless they are intended to replace those projects or systems.
- Determining which IT investments should be recommended to the Executive Director for Operations as major investments reportable to OMB.

3.1.5 Security Control Test and Evaluation

NRC 2004 OMB FISMA Report A.2.c

FISMA requires agencies to test the management, operational, and technical controls of every information system identified in their inventory no less than annually. OMB has instructed agencies to use NIST SP 800-26 to conduct the annual reviews. NIST SP 800-26 is based on the Chief Information Officer Council's "Federal Information Technology Security Assessment Framework" (the Framework). The Framework comprises five levels to guide agency assessments of their security programs and assist in prioritizing efforts for improvement. Level 1 reflects that an asset has documented security policy. At Level 2, the asset also has documented procedures and controls to implement the policy. For Level 3, procedures and controls have been implemented to protect the asset. Level 4 indicates that procedures and controls are tested and reviewed. Finally, at Level 5, the asset has procedures and controls fully integrated into a comprehensive program.

NRC performs a review of security practices and security controls for each major application and general support system by performing annual self-assessments on the systems. The self-assessments are based on NIST SP 800-26. Carson Associates received draft self-assessments for all seventeen NRC major applications and general support systems, as well as for one of the systems currently in development. The final self-assessments were received on September 15, 2004.

As in previous years, NRC developed a modified version of NIST SP 800-26, and all elements of NIST SP 800-26 were included. Some of the self-assessment questions were re-worded to be clearer and to make them more applicable to NRC's environment, and a few additional questions were added.

3.1.6 Contingency Planning and Testing

NRC 2004 OMB FISMA Report A.2.d, A.2.e

One Contingency Plan Is Not Up-To-Date

Sixteen of the seventeen systems have business continuity plans (BCPs), also referred to as contingency plans. Four of the systems' BCPs should have been updated this fiscal year, as they were more than three years old. Three of the outdated BCPs were updated in FY 2004, and the review team verified and validated the updates. The BCP for the LAN/WAN has not been updated since July 2001. However, separate updates to the BCP were developed as LAN/WAN subsystems were certified and accredited. One of the systems in development, DDMS, also has a contingency plan.

RECOMMENDATION

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

10. Update the NRC Local Area Network/Wide Area Network Business Continuity Plan.

All Contingency Plans Have Been Tested

All sixteen BCPs have been tested in the past fiscal year (one system does not have a BCP). One BCP was tested in the 4th Quarter FY 2003, two were tested in the 2nd Quarter FY 2004, eight were tested in the 3rd Quarter FY 2004, and five were tested in the 4th Quarter FY 2004. The review team verified and validated the majority of the BCP test results, and will verify and validate all of the BCP test results during ongoing POA&M validation.

Critical Infrastructure Protection

NRC's Critical Infrastructure Protection Plan has been updated in accordance with OMB Memorandum M-04-15, *Development of Homeland Security Presidential Directive – 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources*. It includes a review of the agency's operations, functions, and services. The review concluded that NRC has no national critical operations and services.

3.1.7 System Inventory

NRC 2004 OMB FISMA Report A.3.d, A.3.e

MD 12.5 was updated in September 2003, and additional text was added to clarify who is responsible for developing and maintaining the system inventory. The CIO is responsible for developing and maintaining an annual inventory of NRC automated information systems (including major national security systems) operated by or under the control of the agency. The identification of all major information systems in the inventory must include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. Regional Administrators and Office Directors must ensure that information systems sponsored by their office are included in the master inventory maintained by OCIO. System sponsors/owners must ensure that all office-sponsored IT systems are properly categorized and accurately reflected in the master inventory of systems maintained by OCIO. Each office will work with OCIO to update and revalidate the master inventory of systems on an annual basis.

Four categories of systems are to be included on the master inventory: major applications, general support systems, listed systems, and other systems. "Listed" systems were described earlier in *Section 3.1.3, Certification and Accreditation*. MD 12.5 defines "Other" as a system that does not require additional security protections, and the information being processed by the system is adequately protected by the security provided by the NRC LAN/WAN. This categorization assumes that OCIO and the sponsor have first jointly decided that the application is appropriately called a system and is to be included in the NRC master inventory of systems. Systems in the "Other" category are typically collections of computer-based activities that while focused on a particular mission function or objective do not have the structure, size, data sensitivity, or the mission importance to warrant additional special management attention or additional security controls.

As a result of a POA&M item from the FY 2003 FISMA review, the agency issued a memorandum in November 2003 asking NRC offices to provide input to OCIO for updating the agency's list of systems. The request was combined with a request from the Office of the Chief Financial Officer for an update of the cost for internal use software. The two requests were combined in order to minimize the impact on NRC offices. The memorandum states that in the future, OCIO and the Office of the Chief Financial Officer will be issuing two calls per year to update/validate the data. The memorandum included as an attachment a list of systems for each office. Offices were requested to review and update the information as necessary, and provide inputs by December 15, 2003. The next request was sent in August 2004.

NRC uses the Information Technology Systems Security Tracking System (ITSSTS) to maintain their system inventory. Their inventory includes not only major applications and general support systems, but also listed and other systems. Carson Associates also reviewed a system inventory report from ITSSTS (by office by system) dated August 4, 2004, and it includes a total of five general support systems, fourteen major applications, 153 listed systems, and 273 other systems.

As a result of a POA&M item from the FY 2003 FISMA review, the agency also began maintaining a list of interfaces for some of their systems. This list is maintained by a contractor supporting OCIO and is not a part of ITSSTS.

The OIG is not involved in the development of the agency's major IT system inventory. However, the OIG is involved in verification of the inventory as a part of the annual FISMA review of the agency's information security program.

3.1.8 E-Authentication

NRC 2004 OMB FISMA Report A.3.h

In accordance with OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, NRC has begun assessing systems for e-authentication risk. A contract was awarded in the 3rd Quarter FY 2004 and NRC is on track to meet the December 15, 2004, deadline for classifying all major applications.

3.1.9 Senior Agency Information Security Officer

NRC 2004 OMB FISMA Report A.3.i

FISMA requires the CIO of each Federal agency to designate a senior agency information security officer who shall carry out the CIO's responsibilities described in FISMA; possess professional qualifications, including training and experience, required to administer the functions described in FISMA; have information security duties as that official's primary duty; and head an office with the mission and resources to assist in ensuring agency compliance with FISMA.

For the past two years, OMB has asked agencies to report whether they have appointed a senior information security officer who reports to the agency CIO, even though FISMA does not specifically state that the official should report to the CIO.

NRC's Senior Information Technology Security Officer (SITSO) left the agency in late 2003 and as of December 12, 2003, the Director of the Program Management, Policy Development, and Analysis Staff within OCIO is currently serving as acting SITSO. The agency is in the process of looking for someone to fill the position and anticipates hiring a new SITSO by the end of October 2004.

The former SITSO did not report directly to the CIO, and the new SITSO, once hired, will also not report directly to the CIO. The SITSO will report to the Director of the Program Management, Policy Development, and Analysis Staff within OCIO on day-to-day matters, and will have direct access to the CIO on any computer security issues.

3.2 Assessment of the POA&M Process

NRC 2004 OMB FISMA Report Section C.1

NRC has two primary tools for tracking the progress of corrective actions related to correcting weaknesses identified during the annual agency security review, the OIG independent evaluation, various security documents, and other security studies conducted by or on behalf of the agency. At a high level, NRC uses the POA&M submitted to OMB to track corrective actions from the OIG annual independent evaluation, and the agency's annual review. The POA&M may also include corrective actions resulting from other security studies conducted by or on behalf of NRC.

At a more detailed, level, NRC uses the NRC ITSSTS to track the progress of internal corrective actions (i.e., those not reported to OMB). ITSSTS is used to track more specific corrective actions, such as those resulting from risk assessments, security test and evaluation associated with the certification and accreditation process, and contingency plan testing.

The FY 2003 FISMA independent evaluation of NRC's information security program found that the agency's corrective action tracking process needed improvement and that not all corrective actions resulting from security reviews and testing were being tracked. The OIG recommended that the agency identify all weaknesses and recommendations from security documentation and any other security reviews, and determine in which tool the recommendations will be tracked. In November 2003, OCIO issued a memorandum describing the agency's information technology security action item tracking process, strategy, and tools. The memorandum describes the types of activities that might identify security weaknesses in NRC information technology systems and describes the two tools used by NRC for tracking the process of security corrective actions – the FISMA POA&M and ITSSTS. The memorandum also states that NRC updates the status of all action items in the POA&M and the ITSSTS database at least quarterly, and more frequently as system testing and other security activities are completed.

NRC had made significant progress in correcting weaknesses identified during the FY 2003 FISMA review. However, the corrective action tracking process needs further improvement, as findings and recommendations resulting from security reviews and testing are not consistently being tracked. Carson Associates also found that the agency's POA&M needs improvement.

NRC Has Made Significant Progress in Correcting FY 2003 Weaknesses

The 4th Quarter FY 2003 POA&M submitted to OMB in October 2003 included a few POA&M items carried over from the previous POA&M, plus the new weaknesses identified during the FY 2003 FISMA review. NRC reported a total of 10 program level POA&M items to OMB, and 59 system level items for which corrective action is ongoing.

During FY 2004, NRC added 2 more program level items, and 12 more system level items, for a total of 12 program level items and 71 system level items. During FY 2004, NRC reported as completed a total of 10 program level items, and 59 system level items. There are 2 program level and 12 system level items remaining on the POA&M for which corrective action is ongoing. NRC has completed approximately 83% of the POA&M items on the FY 2004 POA&M submitted to OMB.

Carson Associates, as part of the FY 2004 FISMA review, has been validating closure of program and system level POA&M items as the agency has submitted their quarterly updates. Carson Associates verified and validated closure of all POA&M items reported closed during the 4th Quarter FY 2003, and the 1st Quarter FY 2004. Carson Associates is in the process of validating closure of items reported during the remaining three quarters of FY 2004. Based on the preliminary analysis of documentation supporting closure of these items, Carson Associates will also verify and validate their closure.

The Corrective Action Tracking Process Needs Further Improvement

During the system evaluations, Carson Associates found that findings and recommendations resulting from testing security controls are not consistently being tracked. The following are some examples.

Certification and Accreditation Testing

The risk assessment for one system identified thirteen risks, and the security test and evaluation plan and report identified eight risks. A mitigation plan submitted with the certification and accreditation package for the system combined the risks identified during the risk assessment and security test and evaluation into one list. Carson Associates could not account for four of the risks from the mitigation plan in the current instance of ITSSTS. According to the agency, these four risks were tracked and completed in 2002. At the exit conference held to discuss the findings of the system evaluation, the agency provided documentation supporting their statement that the risks were tracked and completed in 2002 (output from a previous instance of ITSSTS), but only for three of the four risks that could not be accounted for in the current instance of ITSSTS. The agency could not determine why the three risks were not in the current instance of ITSSTS and could not determine why the fourth risk could not be found in any instance of ITSSTS.

The risk assessment for another system identified eight risks. The security test and evaluation report for the system also identified eight risks, however they were not the same eight risks identified in the risk assessment. The two new risks identified during the security test and evaluation are not being tracked in ITSSTS. Subsequent to the exit conference held to discuss

the findings of the system evaluation, the agency provided a report from ITSSTS that included the two missing risks.

The risk assessment for a third system identified nine risks. Subsequent documentation for the system stated that three risks are acceptable, and provided a detailed discussion of corrective actions necessary to mitigate the remaining risks. A project plan proposed a total of sixteen tasks to address the remaining risks, with two tasks stated as recently completed. The project plan also included a detailed discussion of the remaining tasks, and included a timeline for completing the outstanding tasks. The ITSSTS is reporting three of the remaining risks (also referred to as weaknesses) as "Completed," when the project plan indicates that the tasks required to address the three weaknesses have not been completed. The ITSSTS is also reporting three weaknesses as "Scheduled." However, ITSSTS is not tracking the individual tasks required to address the weaknesses. In some instances, more than one task was suggested to close the weakness. By including only the weakness in ITSSTS and not the individual tasks required to address the weakness, the agency is not able to track completion of the individual tasks proposed in the project plan.

Business Continuity Plan Testing

A memorandum summarizing testing of one system's disaster recovery process resulted in five action items, however none of them are being tracked in ITSSTS or in the agency's POA&M submitted to OMB.

The testing of another system's business continuity plan identified four shortcomings, and resulted in three recommendations. The agency is tracking the four shortcomings in ITSSTS, but is tracking the three recommendations in the POA&M submitted to OMB. The three recommendations do not completely correlate to the four shortcomings, so the agency is tracking different things in their tracking systems. Tracking shortcomings (i.e., weaknesses) in one system and recommendations in another could result in weaknesses not being addressed or overlooked, or in recommendations not being corrected on time.

Other reports

The OIG issued two reports in FY 2004 that included recommendations specific to two NRC systems. One report, "Review of NRC's Personnel Security Program," included three recommendations specific to the Integrated Personnel Security System (IPSS). These recommendations were:

- Issue specific data entry guidance to Division of Facilities and Security staff responsible for entering data into IPSS.
- Formalize the ongoing IPSS data cleanup effort by documenting this effort. This documentation should include a discussion of resources assigned to the effort and a timeline for completion.
- Establish and implement a procedure to validate data accuracy at least annually.

None of these recommendations are being tracked in either of the agency's tracking tools. Subsequent to completion of fieldwork, the agency entered the three recommendations into ITSSTS.

The second report, "Audit of the Licensing Support Network," included two recommendations:

- Establish written agreements with each interconnected party detailing minimum security responsibilities for their interconnected system.
- Update the security plan to include information required by OMB Circular No. A-130.

Only the second recommendation, update the security plan, is being tracked in ITSSTS and the agency's POA&M submitted to OMB. Subsequent to completion of fieldwork, the agency entered the two recommendations into ITSSTS, and OCIO notified the OIG that the corrective actions have been completed. However, the recommendations have not been closed by the OIG.

RECOMMENDATION

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

11. Refine the procedures for identifying weaknesses to be tracked in the Information Technology Systems Security Tracking System.

The Agency's POA&M Needs Improvement

There were a few minor problems with the 4th Quarter FY 2003 and 1st Quarter FY 2004 quarterly updates and POA&M submitted to OMB. In both of these quarterly updates, the metrics reported to OMB did not reflect the contents of the corresponding POA&M. Representatives from OCIO could not account for the discrepancies in the metrics and the contents of the POA&M, as the metrics were calculated and submitted by the previous Senior Information Technology Security Officer. The discrepancies in the metrics were not serious enough to report as a weakness in the FY 2004 FISMA Independent Evaluation.

Program level weaknesses corrected between submission of the 3rd Quarter FY 2003 POA&M and the 4th Quarter FY 2003 POA&M were not included in the 4th Quarter FY 2003 POA&M. The omission of weaknesses corrected between the two POA&M submissions made it difficult for the review team to identify weaknesses corrected during the time between June 30, 2003, and October 1, 2003. The difficulty was compounded by inconsistencies in the metrics submitted with the 4th Quarter FY 2003 POA&M. The FY 2004 FISMA guidance 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. FISMA guidance also states that the POA&M should include the date of completion in the Status column. The NRC POA&M does not include completion dates in the Status column, making it difficult to identifying weaknesses that have been completely mitigated for over a year.

There was also a very minor issue with the 2nd Quarter FY 2004 POA&M. Text in column 5 (Milestones with Completion Dates) was changed for every item in the POA&M. No milestone

dates were changed, only the text describing the milestones. Additional text was added to some milestones. While the milestone dates were not changed per OMB guidance, the change to the text describing the milestones made it difficult to verify there were no changes to the milestones. Because of the changes to the text, every milestone had to be carefully reviewed to make sure no dates had been changed. In addition, the wording of the milestones from an action (e.g., Issue revised guidance), to a statement (e.g., Revised guidance issued) almost implies that those activities actually occurred on the dates listed with them.

RECOMMENDATIONS

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

12. Report corrected weaknesses on the POA&M for a year after their completion.

13. Include a completion date in the Status column of the POA&M.

3.3 Assessment of the Certification and Accreditation Process

NRC 2004 OMB FISMA Report Section C.2

MD 12.5 assigns the CIO responsibility for reviewing and approving security certifications and accreditations for NRC information systems, including risk analysis results, security plans, and contingency plans. Regional Administrators and Office Directors are responsible for ensuring the preparation and periodic updates of required system security documentation are completed in order to facilitate the design, implementation, operation and maintenance, testing, and security certification and accreditation of information systems for which their office is the system sponsor.

Part 4 of the MD 12.5 Handbook describes the certification and accreditation process used at NRC. According to MD 12.5, FISMA directs NIST to prescribe standards and guidelines that provide minimum information security requirements and improve the security of Federal information and information systems, and these standards and guidelines are mandatory. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans. MD 12.5 states that NRC shall comply with NIST guidance to include guidance related to the preparation of security documentation (such as system security plans, risk assessments, and contingency plans), and other applicable NIST guidance for information technology security processes, procedures, and testing. OMB guidance states that reviews and evaluations of agency IT security programs and systems should consider adherence to standards and consistency with NIST guidance.

NRC requires the certification and accreditation of all major applications and general support systems, and the C&A package must include the following documentation:

- Risk Assessment Report
- System Security Plan
- Security Test and Evaluation Plan and Report

- Contingency Plan and Contingency Plan Test Report
- Information System Security Officer Appointment Letter
- Certification Report With Certification Signature
- Accreditation Signature

MD 12.5 also describes the certification and accreditation requirements for "listed" and "other" systems on the NRC inventory.

Carson Associates reviewed the certification and accreditation packages for four systems as part of the system evaluations conducted for the FY 2004 FISMA review. Carson Associates found that all systems followed the NRC certification and accreditation process, and the certification and accreditation packages contained all of the required documentation. However, in some cases the documentation was not consistent with NIST guidelines. Carson Associates also found that in some cases, security protection requirements were inconsistent within security documentation. Security test and evaluation conducted on one system as part of the certification and accreditation of the system was not comprehensive and was not performed by an independent party.

Separate system evaluation reports were prepared and delivered to the agency and include recommendations specific to each system. The following findings are for the certification and accreditation process itself and are not specific to any one system.

Security Documentation Is Not Always Consistent With NIST Guidelines

Risk Assessments

One risk assessment did not describe the threat-sources[5] and vulnerabilities[6] identified for the system, and did not describe how risk levels were determined. NIST SP 800-30, *Risk Management Guide*, describes risk as "a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." The risk assessment presented a table summarizing the findings and recommendations, where the second column of the table represented threats. However, the risk assessment did not include a list of potential threat-sources that could exploit system vulnerabilities, did not include a list of potential vulnerabilities applicable to the system, and did not discuss the threat-source/vulnerability pairs that identified the threats listed in the summary table.

NIST SP 800-30 describes risk level as a function of the likelihood of a given threat-source's attempting to exercise a given vulnerability (i.e., the likelihood of the threat), the magnitude of the impact should a threat-source successfully exercise the vulnerability (i.e., the impact of the

[5] A threat-source is either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

[6] The potential for a particular threat-source exercise (accidentally trigger or intentionally exploit) a particular vulnerability is also known as a threat. A vulnerability is a flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

threat), and the adequacy of planned or existing security controls for reducing or eliminating risk. To measure risk, a risk scale and risk-level matrix must be developed. The table in the risk assessment discussed in the previous paragraph only presented the risk levels, and did not identify or describe how these risk levels were determined. The risk assessment identified several threats with a "Medium" risk level, but did not describe whether these were threats with high impact or a high likelihood. The controls recommended to mitigate the risk could vary greatly depending on which factor (likelihood or impact) contributed the most to the risk level. Understanding likelihood and impact is also important in prioritizing the implementation of recommended corrective actions.

The risk assessment for another system also had several problems. There were errors in the risk levels in some of the tables of the report. In some cases, a risk level was incorrectly calculated, and in others, the risk level changed from table to table. The final table in the report was missing an entry that was included in all of the previous tables. The risk assessment only recommended security controls that could mitigate or eliminate the identified high and medium level risks, but gave no rationale for excluding recommendations for addressing the low level risks. The risk assessment should provide recommendations for all risks, or a rationale for providing only recommended controls for high and medium level risks.

The recommended controls in the risk assessment were very high level and did not include specific corrective actions to address the identified vulnerabilities. NIST SP 800-30 recommends using vulnerability sources, system security testing, and a security requirements checklist for identifying system vulnerabilities. The methodology needed to identify vulnerabilities varies, depending on the system's phase in the life cycle. The system was in the implementation phase when the risk assessment was conducted. NIST SP 800-30 states that identification of vulnerabilities for systems in this phase should include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation. Questionnaires and interviews with personnel responsible for the system were used to identify technical and non-technical vulnerabilities, resulting in identification of generic technical and non-technical risk controls. The risk assessment stated that more implementation specific recommendations would be offered as part of the security plan. However, the security plan contains no recommendations related to the identified risks.

Security Plans

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that the purpose of a security plan is to provide an overview of the security requirements of the system and describe controls in place or planned for meeting those requirements. NIST SP 800-18 also states that the security plan should fully identify and describe the controls currently in place, or planned for the system.

In order to identify what controls were currently in place for the systems, Carson Associates reviewed and analyzed two other documents in conjunction with the security plans – the self-assessments, and results from security test and evaluation of system controls conducted during the certification and accreditation of the systems. Carson Associates reviewed the FY 2003 self-

assessments in order to identify controls in place for the systems. Any controls marked at least at a Level 3 in the self-assessment are considered to be in place based on the definitions in *Section 3.1.5, Security Control Test and Evaluation*. The FY 2003 self-assessments were reviewed as the agency had only provided drafts of the FY 2004 self-assessments when the fieldwork was conducted.

Carson Associates also reviewed the results of the security test and evaluation of system controls conducted during the certification and accreditation of the systems. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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. Three of the Security Test and Evaluation Plans and Reports included an appendix with test procedure worksheets used to record the results of the testing. The test objectives on the test procedure worksheets correspond to the control objectives in the NIST SP 800-26 self-assessment. Each test objective is marked as either pass, fail, or not applicable. A test objective marked as pass represents a security control that is in place. The format of the Security Test and Evaluation Plan and Report for the fourth system was different from the other three, so only the self-assessment was used to identify security controls in place for that system.

Carson Associates found several areas in the system security plans for all four systems where controls were not described. Carson Associates identified several cases where either the self-assessment and/or the test procedure worksheet indicated a control was in place, but it was not described in the security plan. Carson Associates also identified several instances where the information in the security plan, self-assessment and/or test procedure worksheets was inconsistent. Security plans should describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that passed during security test and evaluation. The self-assessment should also reflect all controls in place. In-place controls are those that passed during security test and evaluation.

Contingency Plans

Carson Associates used NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* to evaluate the contingency plans (referred to as business continuity plans) of the four NRC systems. Carson Associates found that the business continuity plans (BCPs) were consistent with NIST SP 800-34 guidance for the most part, but there were several areas where information was missing, or out of date. The following are some examples:

- Some of the BCPs did not include information on what changes have been made to the plan and when. According to the agency, NRC requires annual updates of all BCPs, however NRC only requires conformance with current NIST guidance at the time of re-accreditation. However, without information on what changes were made and when, Carson Associates could not determine whether the BCPs that were reviewed were updated as part of the annual requirement, or as part of a system re-accreditation. NIST SP 800-34 states that the contingency plan should be a living document that is changed as required to reflect system, operational, or organizational changes. Modifications made to

the plan should be recorded in a record of changes, which lists the page number, change comment, and date of change.

- The personnel contact information in some of the BCPs was not up-to-date and did not include notification procedures or contact information for notifying personnel during non-business hours. In some cases, the BCPs did not include personnel contact information for team leaders, alternate team leaders, or team members. Not having up-to-date contact information to reach the designated teams during both business and non-business hours may cause delays in the disaster recovery process.
- Some BCPs did not include procedures for restoring system operations that include procedures for cleaning the alternate site of any equipment or other materials belonging to the organization, with a focus on handling sensitive information. These procedures are necessary to ensure that no sensitive materials remain at the alternate site.

RECOMMENDATION

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

14. Develop a process for ensuring security documentation supporting system certification and accreditation is consistent with NIST guidelines.

Security Protection Requirements Are Inconsistent Within Security Documentation

FISMA defines the term "information security" to mean protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Confidentiality is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Integrity is guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Availability is ensuring timely and reliable access to and use of information. Confidentiality, integrity and availability are often referred to as security protection requirements or security objectives for a system.

Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires all Federal agencies to categorize their systems by assigning potential impact levels to the three security objectives. The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.[7] The potential impact is moderate (medium) if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

[7] Adverse effects on individuals may include, but are not limited to, loss of the privacy to which individuals are entitled under law.

Three of the four systems had different security protection requirements in their security plans and the self-assessments. The protection requirements should be consistent across the security documentation for a system. A change in protection requirements could indicate a need to re-evaluate the risks to the system, especially if the change is from a lower rating to a higher one. If the protection requirements have changed since the system's security plan was finalized, then an explanation for the change should be noted on the self-assessment.

RECOMMENDATION

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

15. Develop a process for ensuring security protection requirements (confidentiality, integrity, availability) are consistently defined in security plans and self-assessments.

Security Test and Evaluation for One System Was Not Comprehensive and Not Independent

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, states that "Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, 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." The security test and evaluation plans and reports for three of the four systems demonstrated that comprehensive testing was performed on the security controls of those systems. However, the security test and evaluation conducted on the fourth system was not comprehensive and was not performed by an independent party.

The test scenarios used in the system's security test and evaluation plan only tested user authentication, user logon, password management, user logoff, user profiles and user groups. While this type of testing may be appropriate as a part of the life cycle testing performed during the implementation phase, it is not appropriate for security test and evaluation associated with certification of a system.

NIST SP 800-30 recommends using vulnerability sources, system security testing, and developing a security requirements checklist for identifying system vulnerabilities. The methodology needed to identify vulnerabilities varies, depending on the system's phase in the life cycle. The system was in the implementation phase when the risk assessment was conducted. NIST SP 800-30 states that identification of vulnerabilities for systems in this phase should include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation. Questionnaires and interviews with personnel responsible for the system were used to identify technical and non-technical vulnerabilities, resulting in identification of generic technical and non-technical risk controls. However, the risk assessment did not identify any actual threats/vulnerabilities to the system, therefore, it is essential that the security test and evaluation include a comprehensive assessment of management, operational, and technical controls. For example, the risk assessment identified the environment in which the system is installed as a potential vulnerability. The security test and evaluation did not test any physical controls.

The security test and evaluation plan described the process the tester should follow when failures or problems are found – after the problem is resolved, the correction is tested again. If the failure or problem is found during integration or system testing, then regression testing is also supposed to be performed. However, there are several tests that appear to have been recorded first as a fail, then changed to a pass. None of the pages where failures appear to be noted have an indication of what caused the test to fail, what corrections (if any) were made to the system to correct the error, and when the test was repeated after the correction was made.

The contractor who developed the system performed the security test and evaluation. This is contrary to guidance in NIST SP 800-37. To preserve the impartial and unbiased nature of the security certification, the certification agent should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system. The certification agent should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of the certification agent is an important factor in assessing the credibility of the security assessment results and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based, accreditation decision. When the potential agency-level impact is moderate or high, certification agent independence is needed and justified.

RECOMMENDATION

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

16. Develop a process for ensuring security test and evaluation in support of certification and accreditation is comprehensive and independent.

3.4 Security Configurations and Patching

NRC 2004 OMB FISMA Report Section D

The CIO has implemented several policies that address security configurations and their implementation. The CIO developed a NRC System Security Baseline Implementation Plan, with an objective to establish, develop, implement, maintain, and verify secure baseline configurations for all information systems. The NRC program is based on Center for Internet Security Benchmarks and Scoring Tools. NRC personnel compiled and researched recommended "best practice" technical settings and actions and developed "in house" benchmarks for those platforms for which a benchmark has yet to be developed. The following platforms are the focus of the initiative:

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

- Linux

Follow-up initiatives will address upcoming operating systems (e.g., Windows XP), and lesser-utilized operating systems, specific applications (e.g., web servers), networking infrastructure devices (e.g., routers), and other miscellaneous systems and devices (e.g., wireless). The scope of the plan is all NRC systems running operating systems listed above and includes all systems that are currently in an "active" state and are components of the primary NRC LAN/WAN.

The plan describes the methodology as comprising four steps:

- Benchmark definition – NRC is using Center for Internet Security terminology for benchmarks – Level-I and Level-II, with Level-II being more secure. The goal for the initiative is to have NRC systems satisfy Level-I benchmark criteria.
- Identification of security benchmarks – NRC has identified six initial benchmarks as described earlier.
- Security benchmark implementation – Only systems running one of the six operating systems described earlier are covered by the initiative. The plan also discusses plans for ensuring a Benchmark compliant desktop image.
- Scoring tools and system reviews – The scoring tools must be installed on each system that it will be run against. Automated tools have not yet been selected/developed for IBM AIX or Novell NetWare, so manual system reviews will be required. The minimum scoring tool score for any NRC system should be a seven. After NRC system administrators have implemented the security benchmarks, a sample of representative systems will be selected to verify that baseline configurations are not only completed, but also completed satisfactorily.

The plan states that, while the goal is to score at least a seven, ideally, every NRC system should score a ten unless a valid operational reason or justification can be provided. The plan also states that different systems have different operational requirements, and the decision may be made to leave certain services running or not to configure certain security parameters. This is acceptable, as long as informed decisions are being made to deviate from the established benchmark. Appendix A of the plan contains a list of NRC servers requiring security baseline implementation.

Carson Associates reviewed a Security Benchmark Compliance Tracking report that tracks NRC system administrator progress towards implementing secure operating system benchmarks on NRC servers, and determining system compliance with benchmarks through the reporting of benchmark scoring tool results. The document includes a compliance tracking table that lists the scores for servers that have had benchmarks applied to them. The document discusses concerns administrators had with trying to score at least a seven on their benchmark implementation. The document states that a score of seven was arbitrarily selected so that administrators would strive to make systems as secure as possible. If it is determined that the best score obtainable for a system in its given environment is a five, then that is acceptable, as long as explanation as to why a five is the best score is provided. The review team compared the table in the document to Appendix A of the NRC System Security Baseline Implementation Plan, and found that the

majority of the servers initially identified as requiring security baseline implementation have had it completed.

In addition to the six benchmarks NRC is currently using, NRC is also using industry guidelines for establishing baselines for Microsoft Internet Information Server and Microsoft SQL Server. National Security Agency guidelines are being used to "harden" new boxes running either of these services. The next "platform" NRC plans to focus on is the Citrix servers. The Citrix vendor came in as part of a pilot project and deployed new Citrix servers. The vendor provided documents on Citrix best practices for securing Citrix servers. The servers also went through the Consolidated Test Facility standard auditing process.

For desktops, NRC has developed a standard image for Windows XP, based on NIST best practices. The majority of desktops at NRC are Windows NT and are being upgraded to Windows XP. NRC uses workstation upgrades that are "pushed" at login to keep Windows NT desktop configurations consistent across NRC. LANDesk can also be used to push upgrades to the desktops. Network bulletins are used to announce agency workstation updates. The bulletins describe the nature of the upgrade, and that it will occur using an automated procedure that will occur during network login. The bulletin includes, as an attachment, the schedule of when the upgrade will take place for each office in NRC.

NRC currently has only one Windows 2003 server. The Windows 2000 best practices were used to "harden" this server, as there are not any established baselines for Windows 2003 available. For the Cisco routers, NRC used the Router Audit Tool. The "hardening" was done only once, when the LAN/WAN was certified and accredited. NRC policy for routers is that once the configuration is set, as long as it stays the same, they do not need to be audited on a periodic basis.

NRC developed system security screening guidelines for preparing new systems for implementation into the NRC production operating environment. The security screening ensures that the system configuration meets NRC LAN/WAN security requirements. The guidelines outline the steps necessary to request and perform the security screening process, guidance on managing and developing a secure system, and industry best practices and additional resources. The review team evaluated Security Screening Forms, results from scoring tools, results from the Microsoft Baseline Security Analyzer, and results from system scans for a few servers and found that the system security screening guidelines are being followed.

The benchmarks used at NRC include checks for the latest patches. The Microsoft Security Baseline Analyzer, which is also used when "hardening" Windows servers, also checks for the latest patches. The process for implementing changes to servers described above also addresses patching of security vulnerabilities.

3.5 Incident Detection and Handling Procedures, and Incident Reporting and Analysis

NRC 2004 OMB FISMA Report Section E and F

NRC's Information Systems Security Incident Response Procedures define the procedures for reporting incidents internally, for external reporting to law enforcement, and for reporting to the United States Computer Emergency Readiness Team (US-CERT)[8]. The procedures define the roles and responsibilities of the Computer Security Incident Response Capability – a team of highly skilled and knowledgeable NRC staff responsible for responding to computer security incidents.

The procedures for reporting and responding to information systems security incidents include procedures for:

- NRC employees and system users
- The general public
- Help Desk personnel
- NRC OCIO Network Operations Center
- LAN/WAN Information System Security Officer and Computer Security Incident Response Capability Team
- Director, OCIO, Infrastructure Computing Operations Division

The procedures define reporting requirements for security incidents on a daily, weekly, and monthly basis. The NRC LAN/WAN Information System Security Officer (ISSO) develops a monthly report to send US-CERT on incidents at NRC. The procedures include contact information for notifying US-CERT about security incidents.

The NRC uses severity levels to categorize information security incidents. These labels convey information about the nature and impact of incidents in summary reports and verbal communications. The severity levels do not equate one-for-one with US-CERT priority levels, however the NRC reporting process provides a means to ensure that all required incident information is conveyed to US-CERT in a timely manner. NRC has not had any successful security incidents in FY 2004, other than an occasional virus infection.

NRC uses a variety of tools, techniques, and technologies to mitigate IT security risk. NRC uses network vulnerability assessment tools to perform scans of critical systems on a periodic basis. NRC has performed external penetration testing of their network and systems, and internal penetration testing is schedule to begin soon. NRC also performs periodic testing for wireless access points (NRC currently does not permit wireless access points, except during pilot tests). Virus detection software is installed on all mail servers and desktops. A critical server supporting the Electronic Information Exchange requires client certificates for access.

NRC uses a cache flow web proxy device to block active content and block access to specific web sites that NRC has identified as inappropriate. All outgoing telnet and file transfer protocol must go through the NRC proxy as well. There is an intrusion detection system at the perimeter and software that can detect unauthorized changes to files has been installed on the NRC web

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

server. OCIO staff members review firewall and intrusion detection logs on a daily basis. Logs from the NRC's web server are also reviewed daily.

NRC is currently piloting a new vulnerability management system that identifies network vulnerabilities and provides extensive flexibility to allow NRC to tailor the vulnerability management process to meet their business requirements in addition to their network security needs.

3.6 Security Awareness and Training

NRC 2004 OMB FISMA Report Section G

All new NRC employees receive computer security orientation when they begin employment at the agency. This orientation program consists of an oral presentation and a video. A member of the computer security staff also talks to the new personnel. Annual computer security training has been mandated for all employees since 1987 and is provided via an on-line ten-part security awareness course. OCIO maintains a database of personnel who have taken the security awareness course and cross checks the list on a regular basis with an employee list provided by NRC Human Resources. A member of the computer security staff sends a message to offices around the first of the month reminding them to have their employees take the course.

NRC's online computer security training courses were updated in FY 2004 to reflect the latest guidance from FISMA. A network announcement was distributed and all employees and contractors with IT system access have begun taking the updated course. FISMA requires that the computer security awareness course be completed annually. NRC also conducted its annual "Computer Security Awareness Day" on November 20th, 2003. Over 200 employees and contractors attended the guest speaker's presentation, and approximately 650 individuals visited booths in the Exhibit Hall.

Positions with significant security responsibilities are defined with qualifications criteria, and the responsibilities are documented in position descriptions. OCIO maintains a list of all personnel with specialized security responsibilities, such as the ISSOs formally appointed for each of the applications and systems. ISSOs must sign an acknowledgement of their responsibilities when taking the position. All ISSOs are required to take an on-line ISSO training course in addition to the on-line security awareness course.

In addition to the on-line courses, the agency uses Yellow Announcements to remind employees of NRC information technology security policies. Recent Yellow Announcements include topics such as the use of the Internet at NRC, misuse of agency computers, the Privacy Act at NRC, and interim guidance for Official Use Only Information. The agency also uses network bulletins sent via e-mail to alert employees of potential security concerns. For example, employees were recently warned about suspicious e-mails requesting CitiBank account information. Security awareness articles are frequently published in NRC's newsletter and OCIO holds occasional seminars on security topics, such as the spam seminar held in July 2004.

Agency staff and contractors are advised of the dangers of peer-to-peer applications during their annual web based security training. The on-line security awareness course includes a discussion

of the dangers of peer-to-peer applications such as instant messaging and there are plans to address the subject in more detail in the next version of the on-line security awareness course. Agency policy does not explicitly prohibit peer-to-peer applications, however the agency's firewall policy does indicate that there should be no non-proxied connection from the agency without explicit approval. Currently certain firewall filters have been put in place to block specific peer-to-peer applications. While some peer-to-peer applications may be able to traverse the firewall, new filters are created to combat these connections as the connections are discovered. The new firewall, planned for implementation in September 2004 will allow peer-to-peer applications to be blocked more easily. One type of instant messaging is permitted in one of NRC's regions to provide Section 508 support for an employee.

NRC is currently developing a security awareness and training plan in accordance with Office of Personnel Management final regulations concerning information technology security awareness (5 CFR Part 930, Subpart C, effective June 14, 2004).

4 Consolidated List of Recommendations

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

1. Remove sensitive data from Management Directive 12.5, *NRC Automated Information Security Program*, which should not be disclosed to the public.
2. Update the Security Services Agreement between the Department of the Interior National Business Center and NRC to include a requirement to exchange relevant system security plans.
3. Develop a Service Level Agreement and Interconnect Security Agreement between the Department of the Interior National Business Center and NRC as described in the DOI Evaluation Report, "Review of Information System Security over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of the Interior Clients."
4. Update the Service Level Agreement between NRC and the National Institutes of Health.
5. Re-certify and re-accredit the NRC Data Center/Telecommunications System.
6. Re-certify and re-accredit the NRC Local Area Network/Wide Area Network.
7. Re-certify and re-accredit the Emergency Response Data System.
8. Re-certify and re-accredit the Emergency Telecommunications System.
9. Update the NRC Local Area Network/Wide Area Network Risk Assessment.
10. Update the NRC Local Area Network/Wide Area Network Business Continuity Plan.
11. Refine the procedures for identifying weaknesses to be tracked in the Information Technology Systems Security Tracking System.
12. Report corrected weaknesses on the POA&M for a year after their completion.
13. Include a completion date in the Status column of the POA&M.
14. Develop a process for ensuring security documentation supporting system certification and accreditation is consistent with NIST guidelines.
15. Develop a process for ensuring security protection requirements (confidentiality, integrity, availability) are consistently defined in security plans and self-assessments.
16. Develop a process for ensuring security test and evaluation in support of certification and accreditation is comprehensive and independent.

5 OIG Response to Agency Comments

On September 22, 2004, the Executive Director for Operations provided comments concerning the draft Independent Evaluation Report and NRC 2004 OMB FISMA Report. We modified the reports as we determined appropriate in response to these comments.

SCOPE AND METHODOLOGY

The scope of this independent evaluation of the U.S. Nuclear Regulatory Commission (NRC) information security program included:

- NRC major applications and general support systems
- NRC local area network/wide area network equipment
- Information technology equipment supporting NRC systems

The independent evaluation did not include controls related to the management of safeguards or classified information.

To accomplish the independent evaluation objectives, the independent evaluation team conducted interviews with Office of the Chief Information Officer staff members, and NRC system owners. The team reviewed documentation provided by NRC including risk assessments; security plans; contingency plans; security test and evaluation plans and reports; certification and accreditation reports; and other security reviews conducted by or on behalf of NRC.

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

- National Institute of Standards and Technology standards and guidelines
- U.S. Nuclear Regulatory Commission Management Directive 12.5, *NRC Automated Information Systems Security Program*
- NRC Office of the Inspector General Audit Guidance

This work was conducted between June 2004 and September 2004. The work was conducted by Jane Laroussi, Virgil Isola, Anthony Van Dyck, and Diane Reilly from Richard S. Carson & Associates, Inc.

[Page intentionally left blank]

NRC 2004 OMB FISMA REPORT

Office of Management and Budget Memorandum M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*, instructs each agency and agency Inspector General to provide responses for each of the performance measures in a Microsoft Excel spreadsheet reporting template that was provided as Section E of the Memorandum. This appendix presents the performance measures prepared by the Richard S. Carson Associates, Inc., on the behalf of the U.S. Nuclear Regulatory Commission Office of the Inspector General.

[Page intentionally left blank]

2004 FISMA Report

Agency:	Nuclear Regulatory Commission
Date Submitted:	09/24/2004
Submitted By:	OIG

Contact Information:

Name:	Vicki Foster
E-mail:	vxf@nrc.gov
Phone:	(301) 415-5909

To enter data in allowed fields, use password: fisma

Section A: System Inventory and IT Security Performance
NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FY04. NIST 800-26, is to be used as guidance for these reviews.

A.2. For each part of this question, identify actual performance in FY04 for the total number of systems by bureau (or major agency operating component) in the format provided below.

	A.1						A.2									
	A.1.a. FY04 Programs		A.1.b. FY04 Systems		A.1.c. FY04 Contractor Operations or Facilities		A.2.a. Number of systems certified and accredited		A.2.b. Number of systems with security control costs integrated into the life cycle of the system		A.2.c. Number of systems for which security controls have been tested and evaluated in the last year		A.2.d. Number of systems with a contingency plan		A.2.e. Number of systems for which contingency plans have been tested	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
NRC	1	1	17	4	7	3	17	100.0%	17	100.0%	16	94.1%	16	94.1%	16	94.1%
Agency Total	**1**	**1**	**17**	**4**	**7**	**3**	**17**	**100.0%**	**17**	**100.0%**	**16**	**94.1%**	**16**	**94.1%**	**16**	**94.1%**

Comments:

Thirteen of the systems are major applications, and four are general support systems. NRC also has two major applications in development, for a total of 19 systems. Three of the systems are operating under an interim accreditation. The OIG reviewed 4 major applications in detail. Of the 7 contractor operations or facilities, OIG reviewed 2 in conjunction with the system reviews, and reviewed a recent network security testing report for another.

A.3	
A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.	
Statement	**Evaluation**
a. Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.	Almost Always, or 96-100% of the time
b. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide, 800-26.	Frequently, or 71-80% of the time
c. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide.	Almost Always, or 96-100% of the time
d. The agency maintains an inventory of major IT systems and this inventory is updated at least annually.	Almost Always, or 96-100% of the time
e. The OIG was included in the development and verification of the agency's IT system inventory.	Almost Always, or 96-100% of the time
f. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities.	Almost Always, or 96-100% of the time
g. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency.	Almost Always, or 96-100% of the time
Statement	**Yes or No**
h. The agency has begun to assess systems for e-authentication risk.	Yes
i. The agency has appointed a senior agency information security officer that reports directly to the CIO.	Yes

Comments:

b. NRC uses NIST SP 800-26 for reviewing their own programs and systems, however NRC primarily uses methods other than NIST SP 800-26 for reviewing contractor operations and facilities. NRC presumes that that two agencies supporting NRC are also following FISMA and NIST guidelines, and there are agreements in place with the 2 Federal agencies. For contractors and commercial entities providing services, NRC includes security requirements in contract language.

e. The OIG does not participate in the development of the agency's major IT system inventory, but does verify the inventory is accurate and up to date.

i. NRC's SITSO left the agency in late 2003 in late 2003, and as of December 12, 2003, the Director of the Program Management, Policy Development, and Analysis Staff within the Office of the Chief Information Officer is currently serving as acting SITSO. The agency is in the process of looking for someone to fill the position and anticipates hiring a new SITSO in the next 60 days. The former SITSO did not report directly to the CIO, and the new SITSO, once hired, will also not report directly to the CIO. The SITSO will report to the Director of the Program Management, Policy Development, and Analysis Staff within the Office of the Chief Information Officer on day-to-day matters, and will have direct access to the CIO on any computer security issues.

Section B: Identification of Significant Deficiencies
NOTE: ALL of Section B should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row, and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POA&M has been developed. Insert rows as needed.

B.1.

Bureau Name	FY04 Significant Deficiencies			
	Total Number	Total Number Repeated from FY03	Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
NRC	0	0		
Agency Total	0	0		

Comments:

Section C: OIG Assessment of the POA&M Process
NOTE: Section C should *ONLY* be completed by the OIG. The CIO should leave this section blank.
To enter data in allowed fields, use password: fisma

C.1. Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.

C.1	
Statement	**Evaluation**
a. Known IT security weaknesses, from all components, are incorporated into the POA&M.	Almost Always, or 96-100% of the time
b. **Program officials** develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness.	Almost Always, or 96-100% of the time
c. Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	Almost Always, or 96-100% of the time
d. **CIO** develops, implements, and manages POA&Ms for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	Almost Always, or 96-100% of the time
e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always, or 96-100% of the time
f. The POA&M is the authoritative agency **and** IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	Almost Always, or 96-100% of the time
g. System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11).	Almost Always, or 96-100% of the time
h. OIG has access to POA&Ms as requested.	Almost Always, or 96-100% of the time
i. OIG findings are incorporated into the POA&M process.	Almost Always, or 96-100% of the time
j. POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always, or 96-100% of the time

Comments:

The CIO maintains an internal tracking system used as a POA&M tool for tracking security weaknesses of all NRC systems, not just those owned by CIO. Program officials are still responsible for providing inputs to the tracking system, for correcting weaknesses, and for providing updates to CIO. CIO uses a separate POA&M to track weaknesses reported to OMB on a quarterly basis.

C.1 OIG Assessment of the Certification and Accreditation Process
Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process. Comments: The OIG reviewed the C&A packages for four systems as part of the system evaluations conducted for the FY 2004 FISMA review. All systems followed the NRC C&A process, which is based on NIST guidance. All of the C&A packages for the systems that were reviewed contained all of the required documentation (i.e., risk assessment, security plan, security test and evaluation plan and report, contingency plan, contingency plan test report, ISSO appointment memo, certification report with certification signature, and accreditation signature). However, in some cases the documentation was not consistent with NIST guidelines, and in some cases, security protection requirements (confidentiality, integrity, availability) were inconsistent within security documentation. Security test and evaluation conducted on one system as part of the C&A of the system was not comprehensive and was not performed by an independent party.	Good

Section D
NOTE: ALL of Section D should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. **For example:** If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration controls are implemented, the answer would reflect "yes" and "51-70%". If appropriate or necessary, include comments in the Comment area provided below.

D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below.

D.1. & D.2.

	Yes, No, or N/A	Evaluation
D.1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the degree by which the configurations are implemented?	**Yes**	
a. Windows XP Professional	Yes	Almost Always, or 96-100% of the time
b. Windows NT	Yes	Almost Always, or 96-100% of the time
c. Windows 2000 Professional	N/A	
d. Windows 2000	Yes	Almost Always, or 96-100% of the time
e. Windows 2000 Server	Yes	Almost Always, or 96-100% of the time
f. Windows 2003 Server	Yes	Almost Always, or 96-100% of the time
g. Solaris	Yes	Almost Always, or 96-100% of the time
h. HP-UX	No	
i. Linux	Yes	Almost Always, or 96-100% of the time
j. Cisco Router IOS	Yes	Almost Always, or 96-100% of the time
k. Oracle	N/A	
l. Other. Specify: Novell, AIX	Yes	Almost Always, or 96-100% of the time
	Yes or No	**Evaluation**
D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security vulnerabilities?	Yes	Almost Always, or 96-100% of the time

Comments:

Section E: Incident Detection and Handling Procedures
NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.

E.1

Statement	Evaluation
a. The agency follows documented policies and procedures for reporting incidents internally.	Almost Always, or 96-100% of the time
b. The agency follows documented policies and procedures for external reporting to law enforcement authorities.	Almost Always, or 96-100% of the time
c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov	Almost Always, or 96-100% of the time

E.2.

E.2. Incident Detection Capabilities.

	Number of Systems	Percentage of Total Systems
a. How many systems underwent vulnerability scans and penetration tests in FY04?	14	82%

b. Specifically, what tools, techniques, technologies, etc., does the agency use to mitigate IT security risk?

Answer:

Network vulnerability assessment tools, external penetration testing, internal penetration testing scheduled to begin soon. Testing for wireless access points. Virus detection software on all mail servers & desktops. Cache flow web proxy device to block active content & block access to specific web sites. Intrusion detection system at the perimeter. Firewall, intrusion detection, and web logs reviewed on a daily basis.

Comments:

NRC conducts vulnerability scans and penetration tests on portions of their network and not on specific individual NRC systems. Some servers supporting NRC systems were scanned when their operating systems were upgraded (part of NRC's process for putting new servers into production). External penetration testing of NRC's network was conducted in FY 2004. Two NRC systems, and portions of a third, are not housed at NRC, and were not included in any scanning or penetration testing conducted by NRC.

Section F: Incident Reporting and Analysis
NOTE: ALL of Section F should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

F.1. For each category of incident listed: identify the total number of successful incidents in FY04, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VII, "Other". If appropriate or necessary, include comments in the Comment area provided below.

F.2. Identify the **number of systems** affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area provided below.

F.1., F.2. & F.3.

	F.1. Number of Incidents, by category:			F.2. Number of systems affected, by category, on:		
	F.1.a Reported internally	F.1.b. Reported to US-CERT	F.1.c. Reported to law enforcement	F.2.a. Systems with complete and up-to-date C&A	F.2.b. Systems without complete and up-to-date C&A	F.2.c. How many successful incidents occurred for known vulnerabilities for which a patch was available?
	Number of Incidents	Number of Incidents	Number of Incidents	Number of Systems Affected	Number of Systems Affected	Number of Systems Affected
I. Root Compromise	0	0	0	n/a	n/a	n/a
II. User Compromise	0	0	0	n/a	n/a	n/a
III. Denial of Service Attack	0	0	0	n/a	n/a	n/a
IV. Website Defacement	0	0	0	n/a	n/a	n/a
V. Detection of Malicious Logic	33449	33449	0	n/a	n/a	n/a
VI. Successful Virus/worm Introduction	93	93	0	n/a	n/a	n/a
VII. Other	0	0	0	n/a	n/a	n/a
Totals:	33542	33542	0	0	0	0

Comments:

NRC's reporting of security events changed in December 2003. In the 1st 2 months of FY 2004, NRC reported on 12 types of suspicious activity, and categorized the events based on a 5 level system. Level 1 events are observations, level 2 - warnings, level 3 - alerts, level 4 - damage, and level 5 - exploits. For the purposes of reporting successful incidents, only level 3 and higher events would be considered successful. In the 1st 2 months of FY 2004, no level 3 or higher events were reported. Starting in December 2003, NRC's reports include eight types of events that reflect the eight event types reported in US-CERT statistics. Categories V and VI were not tracked in NRC reports for October and November 2003. Detection of malicious logic is considered to be viruses/worms detected at the agency's mail gateway, and by virus detection software on servers and workstations. Successful virus/worm introduction are those that were not detected, and had to be cleaned. Only workstations (no servers) had any actual "infections."

Section G: Training
NOTE: ALL of Section G should be completed by BOTH the Agency CIO and the OIG.
To enter data in allowed fields, use password: fisma

G.1. Has the agency CIO ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? If appropriate or necessary, include comments in the Comment area provided below.

G.1.

G.1.a. Total number of employees in FY04	G.1.b. Employees that received IT security awareness training in FY04, as described in NIST Special Publication 800-50		G.1.c. Total number of employees with significant IT security responsibilities	G.1.d. Employees with significant security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16		G.1.e. Briefly describe training provided	G.1.f. Total costs for providing IT security training in FY04 (in $'s)
	Number	Percentage		Number	Percentage		
3,468	3,023	87.2%	34	32	94.1%	Security awareness training course required for all employees, taken annually. ISSO training course.	$46,300

G.2.

	Yes or No
a. Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?	Yes

Comments:

Total number of employees as of September 21, 2004. The number of employees includes NRC employees and contractors with LAN accounts vs. all employees at NRC. Only employees and contractors with LAN accounts are required to take awareness training.