Systems Evaluation of the Fees Systems

OIG-04-A-23 September 30, 2004

REDACTED FOR PUBLIC RELEASE

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

Systems Evaluation of the
Fee Systems

OIG–04-A-23 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

Jesse L. Funches
Chief Financial Officer

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

SUBJECT: SYSTEM EVALUATION OF THE FEE SYSTEMS
(OIG-04-A-23)

This evaluation was conducted as part of the Office of the Inspector General's review of NRC's implementation of the Federal Information Security Management Act (FISMA) for FY 2004. Richard S. Carson & Associates, Inc., performed this independent system evaluation on behalf of OIG.

Based on its review and evaluation of the Fee Systems' management, operational, and technical controls, Richard S. Carson & Associates, Inc., determined that the Fee Systems has the following weaknesses:

- Security documentation does not always follow required guidelines.
- NRC is not tracking all action items resulting from testing the security controls.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on September 14, 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
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

"Office of the Inspector General System Evaluation of the Fee Systems"

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

September 24, 2004

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

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 (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include an independent evaluation of an agency's information security program and practices, 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. As part of the Fiscal Year 2004 FISMA independent evaluation of the U.S. Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the Fee Systems[1].

NRC is required to recover a major portion of its annual budget, and in order to implement this requirement NRC assesses fees in compliance with Federal law and NRC regulations. The primary function of the Fee Systems is to generate invoices to licensees for annual fees and fees for various services, including new licensing approvals, licensing amendments, topical reports, and inspections. Additional functionality includes the tracking of new small-materials licensing application fee payments.

PURPOSE

The system evaluation objectives were to review and evaluate the management, operational, and technical controls for the Fee Systems.

RESULTS IN BRIEF

Carson Associates reviewed the Fee Systems security documentation and found that the Fee Systems security documentation is not always consistent with National Institute of Standards and Technology (NIST) guidelines, and findings and recommendations resulting from testing are not consistently being tracked. None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in Office of Management and Budget guidance.

Security Documentation Is Not Always Consistent With NIST Guidelines

FISMA directs the Secretary of Commerce, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to Federal information systems. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans.

[1] NRC uses the term "Fee Systems" to refer to a group of applications that support the collection of fees from licensees. The group of applications is considered one system for the purposes of FISMA reporting. The term "system" may be used throughout this report to refer to the "Fee Systems."

NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, which was revised in September 2003, 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.

The previous version of MD 12.5 did not require compliance with NIST guidelines, however, Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, states that each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management. OMB periodically reminds agencies that agency security practices should be consistent with NIST guidance. The FY 2004 FISMA guidance issued by OMB specifically states that agencies must follow NIST standards and guidance. Use of NIST guidance is flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance.

Carson Associates reviewed the Fee Systems Risk Assessment, Security Plan, and Business Continuity Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

Findings and Recommendations Resulting From Testing Are Not Consistently Being Tracked

The FY 2003 FISMA independent evaluation of NRC's information security program found that not all corrective actions resulting from security reviews and testing were being tracked and that the agency's corrective action process needed improvement. The Office of the Inspector General (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, the Office of the Chief Information Officer (OCIO) issued a memo describing the agency's information technology security action item tracking process, strategy, and tools. Carson Associates found that findings and recommendations resulting from testing of the Fee Systems security controls are not consistently being tracked.

RECOMMENDATIONS

This report makes four recommendations to the Chief Financial Officer and two recommendations to the Executive Director for Operations to strengthen management, operational, and technical controls for the Fee Systems. A consolidated list of recommendations appears on page 11 of this report.

AGENCY COMMENTS

On September 14, 2004, the Executive Director for Operations and the Chief Financial Officer provided comments concerning the draft system evaluation report. We modified the report as we determined appropriate in response to these comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

BCP	Business Continuity Plan
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GISRA	Government Information Security Reform Act
ITSSTS	Information Technology Systems Security Tracking System
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OCFO	Office of the Chief Financial Officer
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
SP	Special Publication

[Page intentionally left blank]

TABLE OF CONTENTS

[Page intentionally left blank]

1 Background

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 (FISMA) of 2002[2]. FISMA outlines the information security management requirements for agencies, which include an independent evaluation of an agency's information security program and practices, 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. As part of the Fiscal Year 2004 FISMA independent evaluation of the U.S. Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the Fee Systems.

The Fee Systems

NRC is required to recover a major portion of its annual budget, and in order to implement this requirement, NRC assesses fees in compliance with the Omnibus Budget Reconciliation Act of 1990, as amended, and the Independent Offices Appropriation Act of 1952. Fees are recovered as established in 10 CFR Part 170 and 10 CFR Part 171 of NRC regulations. The Office of the Chief Financial Officer (OCFO), Division of Financial Management, License Fee Team administers some components of the License Fee Management Program through use of automated processes. The Fee Systems is a term used to refer to a group of applications that share data from various sources throughout NRC. The group of applications is considered one system for the purposes of FISMA reporting. The term "system" may be used throughout this report to refer to the "Fee Systems."

The primary function of these applications is to generate invoices to licensees for annual fees and fees for various services, including new licensing approvals, licensing amendments, topical reports, and inspections. Additional functionality includes the tracking of new small-materials licensing application fee payments. Two of the Fee Systems applications reside on a mainframe located at the National Institutes of Health (NIH). The remaining applications reside on the NRC local area network.

The NRC OCFO is system owner of the Fee Systems. The Fee Systems have been categorized as a Major Application[3] and are in the operational[4] phase of the system life cycle.

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

[3] An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

[4] A system's life cycle typically comprises five phases: initiation, development/acquisition, implementation, operation/maintenance, and disposal. In the operation/maintenance phase, systems are in place and operating, enhancements and/or modifications to the system are developed and tested, and hardware and/or software is added or replaced.

System Evaluation Process

The Fee Systems were evaluated by reviewing system documentation maintained by the Office of the Chief Information Officer (OCIO). As recommended by the Office of Management and Budget (OMB), Carson Associates reviewed the following documents for adherence to standards and consistency with guidelines issued by the National Institute of Standards and Technology (NIST).

- Fee Systems Risk Assessment, May 2003
- Fee Systems Security Plan, May 2003
- Fee Systems Business Continuity Plan, May 2003
- Fee Systems Security Test and Evaluation Plan and Report, May 2003
- Fee Systems Re-certification and Re-accreditation Report, May 2003
- Fee Systems Remediation Plan, December 2003
- Fee Systems Project Plan, April 2004 and July 2004
- Privacy Impact Assessment
- FY 2003 and draft FY 2004 Fee Systems Self-Assessment

The documents were reviewed to determine whether they are consistent with NIST guidance and whether they describe the management[5], operational[6], and technical[7] controls in place for the Fee Systems.

Carson Associates also reviewed documentation supporting the certification and accreditation of the NIH mainframe to determine whether it is consistent with NIST guidance and whether it describes the management, operational, and technical controls in place for the components of the Fee Systems residing at NIH. Several other NRC systems provide data to the Fee Systems to be used in the generation of invoices. Security controls for these other NRC systems were not analyzed as part of the Fee Systems system evaluation.

2 Purpose

The system evaluation objectives were to review and evaluate the management, operational, and technical controls for the Fee Systems.

[5] The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
[6] The security controls (i.e., safeguards or countermeasures) for an information system that primarily are implemented and executed by people (as opposed to systems).
[7] The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

3 Findings

Carson Associates reviewed the Fee Systems security documentation and found that:

- The Fee Systems security documentation is not always consistent with National Institute of Standards and Technology guidelines.
- Findings and recommendations resulting from testing are not consistently being tracked.

None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in OMB guidance.

3.1 Security Documentation Is Not Always Consistent With NIST Guidelines

FISMA directs the Secretary of Commerce, on the basis of standards and guidelines developed by NIST, to prescribe standards and guidelines pertaining to Federal information systems. NIST has developed several guidelines and standards, including those for conducting risk assessments, developing security plans, and contingency plans. NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, which was revised in September 2003, 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.

The previous version of MD 12.5 did not require compliance with NIST guidelines, however, OMB Circular A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, states that each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce[8], the General Services Administration and the Office of Personnel Management. OMB periodically reminds agencies that agency security practices should be consistent with NIST guidance. The FY 2004 FISMA guidance issued by OMB[9] specifically states that agencies must follow NIST standards and guidance. Use of NIST guidance is flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance.

Carson Associates reviewed the Fee Systems Risk Assessment, Security Plan, and Business Continuity Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

[8] NIST is part of the Technology Administration within the Department of Commerce.
[9] OMB Memorandum M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act, dated August 23, 2004.

Fee Systems Security Plan Does Not Describe All Security Controls Identified As In-Place

OMB A-130 states that security plans shall be consistent with guidance issued by NIST. NIST Special Publication (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. However, Carson Associates found several areas in the Final System Security Plan for the Fee Systems, dated May 2003, where controls were not described.

In order to identify what controls are currently in place for the Fee Systems, Carson Associates reviewed and analyzed two other documents in conjunction with the Fee Systems Security Plan – the Fee Systems self-assessment, and results from security test and evaluation of the Fee Systems controls conducted during the certification and accreditation of the Fee Systems.

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, *Self-Assessment Guide for Information Technology Systems*, 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.

Carson Associates reviewed the FY 2003 Fee Systems self-assessment in order to identify controls in place for the Fee Systems. Any controls marked at least at a Level 3 in the Fee Systems self-assessment are considered to be in place based on the above definitions. The FY 2003 self-assessment was reviewed as the agency had only provided a draft of the FY 2004 self-assessment when the fieldwork was conducted.

Carson Associates also reviewed the results of the security test and evaluation of the Fee Systems controls conducted during the certification and accreditation of the Fee 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. Appendix D of the Fee Systems Security Test and Evaluation Plan and Report, dated May 2003, includes 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.

As a result of the review of the Fee Systems Security Plan, self-assessment, and security test and evaluation results, 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. The following are some examples:

- The Fee Systems Security Plan does not describe tests and examinations of key controls (i.e., network scans, analyses of router and switch settings, penetration testing). However, this control is marked as "pass" on the test procedure worksheets, and is marked as a Level 5 in the Fee Systems self-assessment.
- The Fee Systems Security Plan does not describe how lists of authorized users and their access are maintained and approved. However, this control is marked as a Level 5 in the Fee Systems self-assessment, and is marked as "pass" on the test procedure worksheets.
- The Fee Systems Security Plan does not describe procedures that ensure terminated or transferred individuals do not retain system access. However, this control is marked as a Level 3 in the Fee Systems self-assessment, and is marked as "pass" on the test procedure worksheets.

Carson Associates also identified several instances where the information in the Fee Systems Security Plan, self-assessment and test procedure worksheets is inconsistent. The following are some examples:

- The Fee Systems Security Plan does not describe whether access scripts with embedded passwords are allowed. The Fee Systems self-assessment indicates this control is not applicable, but the control is marked as "pass" on the test procedure worksheets.
- The Fee Systems Security Plan does not describe whether inactive accounts are monitored and if they are removed when not needed. This control is marked as Level 5 in the Fee Systems self-assessment. However, this control is marked as "fail" on the test procedure worksheets.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Chief Financial Officer:

1. Update the Fee Systems Security Plan to describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

2. Update the Fee Systems self-assessment to reflect controls in place. In-place controls are those that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

Fee Systems Business Continuity Plan Is Not Consistent With NIST Guidelines

Carson Associates reviewed the Fee Systems Business Continuity Plan (BCP), dated May 2003. Guidance on developing contingency plans can be found in NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, which was published in June 2002. As recommended by OMB, Carson Associates reviewed the Fee Systems BCP for consistency with NIST guidelines and found that in some instances, the Fee Systems BCP is not consistent with NIST guidelines.

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. This policy is not documented in any agency management directive or in any documentation reviewed by Carson Associates. Carson Associates was informed of this policy during the exit conference held to discuss the findings of the Fee Systems system evaluation. Subsequent to the exit conference, Carson Associates reviewed previous NIST guidance on the preparation of contingency plans, Federal Information Processing Standards (FIPS) Publication 87, *Guidelines for ADP Contingency Planning*, and found that the Fee Systems BCP is also not consistent with the FIPS 87 guidance. As stated earlier in this report, while the version of MD 12.5 that was in effect at the time the Fee Systems BCP was published did not require compliance with NIST guidelines, OMB requires agencies to follow NIST standards and guidance.

OFFICIAL USE ONLY PARAGRAPH REDACTED

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. The Fee Systems BCP does not include any information on what changes have been made to the plan and when. Without this information, Carson Associates could not determine whether the BCP was updated as part of the annual requirement, or as part of a system re-accreditation. FIPS 87 also states that an essential element

of any volatile document, such as a contingency plan, is a method of recording changes to the document.

NIST SP 800-34 suggests including a line of succession that identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so. The line of succession may continue down to the level necessary based on the organization's needs, but must be carefully coordinated with the continuity of operations plan to ensure there are no responsibility conflicts. FIPS 87 also states that the BCP include a section that clearly delineates how the chain of command is to function when an emergency strikes. The Fee Systems BCP does not list the line of succession to assume authority for executing the plan.

NIST SP 800-34 describes roles and responsibilities, including a discussion of appropriate teams to implement the system recovery strategy. Each team should be trained and ready to deploy in the event of a disruptive situation requiring plan activation. Recovery personnel should be assigned to one of several specific teams that will respond to the event, recover capabilities, and return the system to normal operations. The specific types of teams required are based on the system affected. The size of each team, specific team titles, and hierarchy designs depend on the organization. The BCP should include a section describing responsibilities, including the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The section also provides an overview of team member roles and responsibilities in a contingency situation. While FIPS 87 does not include the same level of detail as NIST SP 800-34 in its discussion of the people involved in contingency planning, it does state that is it necessary to associate people, skills and management in recovery. Alternates for persons with peculiar skills or with skills in very short supply must be designated. The Fee Systems BCP includes a list of contacts in Section 1, but the document does not describe the structure and membership of the contingency teams.

NIST SP 800-34 describes notification procedures and states that they should be documented in the plan for both events that occur with and without prior notice. For example, advanced notice is often given that a hurricane will affect an area or that a computer virus is expected on a certain date. However, there may be no notice of equipment failure or a criminal act. The procedures should describe the methods used to notify recovery personnel during business and non-business hours. Prompt notification is important for reducing the effects on the system; in some cases, it may provide enough time to allow system personnel to shut down the system gracefully to avoid a hard crash.

NIST SP 800-34 also states that personnel to be notified in the event of a disaster should be clearly identified in the contact list appended to the plan. The list should identify personnel by their team position, name, and contact information (e.g., home number, work number, pager number, email address, and home address). FIPS 87 also stresses the importance of including the name, address, and phone numbers of all people who may be required in any backup or recovery scenario in the BCP.

However, the personnel contact information in the Fee Systems BCP is not complete and does not include notification procedures or contact information for notifying personnel during non-

business hours. 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.

NIST SP 800-34 describes the fourth step of the contingency process as "develop recovery strategies." Thorough recovery strategies ensure that the system can be recovered quickly and effectively following a disruption. The fifth step is to develop the contingency plan. The contingency plan should contain detailed guidance and procedures for restoring a damaged system. Procedures should be written in a stepwise, sequential format so system components may be restored in a logical manner. The procedures should also include instructions to coordinate with other teams when certain situations occur, such as when an action is not completed within the expected time frame, when a key step has been completed, when item(s) must be procured, or other system-specific concerns.

To facilitate recovery phase operations, the contingency plan should provide detailed procedures to restore the system or system components. Recovery procedures should be written in a straightforward, step-by-step style. To prevent difficulty or confusion in an emergency, no procedural steps should be assumed or omitted. A checklist format is useful for documenting the sequential recovery procedures and for troubleshooting problems if the system cannot be recovered properly.

However, in the Fee Systems BCP, recovery actions are described at a very high level and do not include specific technical details on how to restore a system from backup tapes. While responsibility for restoring the system from backup tapes is primarily the responsibility of other organizations within NRC, the contingency plan should include more details on what steps the System Owner must follow once the system has been restored. For example, the Fee Systems BCP does not include steps for testing system functionality after restoration from backup. In addition, procedures for restoring system operations are not outlined for each team to operate the system in coordination with the system at the original or new site.

NIST SP 800-34 defines the reconstitution phase as when recovery activities are terminated and normal operations are transferred back to the organization's facility. The reconstitution phase should specify teams responsible for restoring or replacing both the site and the system. The Fee Systems BCP does 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. While FIPS 87 does not discuss specific procedures to be followed for cleaning the alternate site of any equipment or other materials belonging to the organization, these procedures are necessary to ensure that no sensitive materials remain at the alternate site.

RECOMMENDATIONS

The Office of the Inspector General recommends that the Chief Financial Officer:

3. Keep copies of the As-Built System Documentation in the same location as the Fee Systems Business Continuity Plan to facilitate access during disaster recovery.

4. Update the Fee Systems Business Continuity Plan to include the following changes:

   - Record modifications to the plan in a record of changes to include what changes were made (e.g., the page numbers or section numbers where the changes were made), why the changes were made (e.g., annual update or update during re-accreditation), and date of change.
   - Include an order of succession that identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so.
   - Include a description of the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The description should include an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.
   - Describe the methods used to notify recovery personnel during business and non-business hours.
   - Include more detailed steps for recovery actions and assign procedures to the appropriate recovery team(s).
   - Include procedures for restoring system operations, with a focus on how to clean the alternate site of any equipment or other materials belonging to the organization.

3.2 Findings and Recommendations Resulting From Testing Are Not Consistently Being Tracked

The FY 2003 FISMA independent evaluation of NRC's information security program found that the agency's corrective action process needed improvement. 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 plan of action and milestones (POA&M) submitted to OMB to track corrective actions from the OIG annual independent evaluation, and the agency's annual review. At a more detailed, level, NRC uses the NRC Information Technology Systems Security Tracking System (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 also found 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 memo describing the agency's information technology security action item tracking process, strategy, and tools. The memo 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 the ITSSTS. Carson Associates found that findings and recommendations resulting from testing of the Fee Systems security controls are not consistently being tracked.

Findings and Recommendations Resulting from the Fee Systems Certification and Accreditation Are Not Consistently Being Tracked

The Fee Systems Risk Assessment identified nine risks. The Fee Systems Remediation Plan, and subsequent Project Plan state that three risks are acceptable, and provide a detailed discussion of corrective actions necessary to mitigate the remaining risks. The Project Plan proposes a total of sixteen tasks to address the remaining risks, with two tasks stated as recently completed. The Project Plan includes a detailed discussion of the remaining tasks, and includes 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, the 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 the 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.

RECOMMENDATIONS

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

5. Update the agency's internal tracking system to reflect the current status of weaknesses identified during the Fee Systems Risk Assessment.

6. Update the agency's internal tracking system to include the individual tasks proposed in the Fee Systems Project Plan to resolve the weaknesses identified during the Fee Systems Risk Assessment.

4 Consolidated List of Recommendations

The Office of the Inspector General recommends that the Chief Financial Officer:

1. Update the Fee Systems Security Plan to describe all controls currently in place. In-place controls are those marked at least at Level 3 in the self-assessment, and that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

2. Update the Fee Systems self-assessment to reflect controls in place. In-place controls are those that were documented as passed in the last Security Test and Evaluation Plan and Report, or in any test and evaluation on controls added since publication of that report.

3. Keep copies of the As-Built System Documentation in the same location as the Fee Systems Business Continuity Plan to facilitate access during disaster recovery.

4. Update the Fee Systems Business Continuity Plan to include the following changes:

   - Record modifications to the plan in a record of changes to include what changes were made (e.g., the page numbers or section numbers where the changes were made), why the changes were made (e.g., annual update or update during re-accreditation), and date of change.
   - Include an order of succession that identifies personnel responsible to assume authority for executing the contingency plan in the event the designated person is unavailable or unable to do so.
   - Include a description of the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams. The description should include an overview of team member roles and responsibilities in a contingency situation. Teams and team members should be designated for specific response and recovery roles during contingency plan activation.
   - Describe the methods used to notify recovery personnel during business and non-business hours.
   - Include more detailed steps for recovery actions and assign procedures to the appropriate recovery team(s).
   - Include procedures for restoring system operations, with a focus on how to clean the alternate site of any equipment or other materials belonging to the organization.

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

5. Update the agency's internal tracking system to reflect the current status of weaknesses identified during the Fee Systems Risk Assessment.

6. Update the agency's internal tracking system to include the individual tasks proposed in the Fee Systems Project Plan to resolve the weaknesses identified during the Fee Systems Risk Assessment.

5 OIG Response to Agency Comments

On September 14, 2004, the Executive Director for Operations and the Chief Financial Officer provided comments concerning the draft system evaluation report. We modified the report as we determined appropriate in response to these comments.

SCOPE AND METHODOLOGY

To perform the Fee Systems system evaluation, Carson Associates reviewed the system's security documentation, including the Security Plan, Risk Assessment, self-assessment, Business Continuity Plan, System Test and Evaluation Plan and Report, Certification and Accreditation documentation, and the completion of weaknesses addressed, if any, within the FY 2003 plan of action and milestones. Comprehensive document checklists were used in the evaluation process. Carson Associates also conducted a phone interview with the Fee Systems System Security Officer.

Carson Associates also reviewed certification and accreditation documentation for the NIH mainframe, which hosts two of the Fee Systems applications.

The work was conducted from June 2004 to August 2004 in accordance with guidelines from the National Institute of Standards and Technology, and best practices for evaluating security controls. Jane Laroussi from Carson Associates conducted the work.