System Evaluation of the Integrated Personnel Security System (IPSS)

OIG-05-A-08 January 14, 2005

REDACTED FOR PUBLIC RELEASE

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

System Evaluation of the Integrated Personnel Security System (IPSS)

OIG-05-A-08 January 14, 2005

EVALUATION REPORT

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

January 14, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: SYSTEM EVALUATION OF THE INTEGRATED PERSONNEL SECURITY SYSTEM (IPSS) (OIG-05-A-08)

Attached is the evaluation report titled*, System Evaluation of the Integrated Personnel Security System (IPSS)*, conducted as part of the Office of the Inspector General's review of the Nuclear Regulatory Commission's (NRC) implementation of the Federal Information Security Management Act (FISMA) for FY 2004. Richard S. Carson & Associates, Inc., performed this independent system evaluation on our behalf.

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

- Security test and evaluation was not comprehensive and was not independent.
- Security documentation is not always consistent with National Institute of Standards and Technology guidelines.
- Security protection requirements are inconsistent within security documentation.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on December 13, 2004, NRC officials provided comments concerning the draft audit report and opted not to submit formal written comments to this final version of the 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
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
Timothy F. Hagan, 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
OPA, Region I
OPA, Region III
OPA, Region IV

Office of the Inspector General
System Evaluation of the
Integrated Personnel Security System (IPSS)

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

December 22, 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 Nuclear Regulatory Commission's (NRC) information technology security program, Richard S. Carson Associates, Inc. (Carson Associates) reviewed security controls for the Integrated Personnel Security System (IPSS).

The Division of Facilities and Security (DFS), Office of Administration, maintains personnel security information on employees in paper files and in an automated data system referred to as the Personnel Security (PERSEC) Modules. In December 2003, DFS implemented a new automated data system, IPSS, to replace the PERSEC Modules. IPSS is intended to be more efficient and user-friendly with more reporting capabilities than the PERSEC Modules, which are viewed as cumbersome and inadequate.

PURPOSE

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

RESULTS IN BRIEF

Carson Associates reviewed IPSS security documentation and found that security test and evaluation was not comprehensive and was not independent, IPSS security documentation is not always consistent with National Institute of Standards and Technology (NIST) guidelines, and the security protection requirements are inconsistent within IPSS security documentation. None of these weaknesses are considered to be significant deficiencies or reportable conditions as defined in Office of Management and Budget (OMB) FISMA reporting guidance.

Security Test and Evaluation Was Not Comprehensive and Was Not Independent

NIST Special Publication 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."

However, the security test and evaluation conducted on IPSS was not comprehensive, the test results were not fully documented, and the testing was not performed by an independent party.

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 developing 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 Governmentwide policies, standards, and procedures issued by OMB, 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 IPSS Risk Assessment Report, System Security Plan, and Contingency Plan and found that while the documentation is up-to-date, it is not always 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. The security protection requirements defined in the IPSS System Security Plan and in the FY 2003 and FY 2004 IPSS self-assessments are inconsistent.

RECOMMENDATIONS

This report makes eight recommendations to the Executive Director for Operations to strengthen management, operational, and technical controls for IPSS. A consolidated list of recommendations can be found on page 15 of this report.

AGENCY COMMENTS

On December 13, 2004, the Executive Director for Operations provided comments concerning the draft system evaluation report. None of the comments required modifications to the report.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

DFS	Division of Facilities and Security
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IPSS	Integrated Personnel Security System
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
OCIO	Office of the Chief Information Officer
OIG	Office of the Inspector General
OMB	Office of Management and Budget
PERSEC	Personnel Security
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.[1] 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 NRC's information technology security program, Carson Associates reviewed security controls for IPSS.

Integrated Personnel Security System

The Division of Facilities and Security (DFS), Office of Administration, maintains personnel security information on employees in paper files and in an automated data system referred to as the PERSEC Modules. In December 2003, DFS implemented a new automated data system, IPSS, to replace the PERSEC Modules. IPSS is intended to be more efficient and user-friendly with more reporting capabilities than the PERSEC Modules, which are viewed as cumbersome and inadequate. IPSS provides DFS with functionality such as:

- Tracking all personnel security processing activities related to the approval or denial of an employment clearance and access authorization.
- Tracking unescorted contractor access to NRC facilities.
- Tracking due process procedures (i.e., denial, revocation, suspension and termination of employment clearance or access authorization).
- Tracking drug testing activities.
- Tracking classified visits to NRC facilities.
- Random selection and tracking of drug program participants.
- Multiple drug testing reports.
- Data consistency, confidentiality, integrity, and authentication.

The Security Branch within the Office of Administration, Division of Facilities and Security is the IPSS system owner. The system is categorized as a Major Application.[2] The IPSS security

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

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

documentation was prepared while the system was still in the implementation phase[3] of its life cycle. IPSS is now in the operational phase.[4]

System Evaluation Process

IPSS was evaluated by reviewing system documentation maintained by the Office of the Chief Information Officer (OCIO). As recommended by OMB, Carson Associates reviewed the following documents for adherence to standards and consistency with guidelines issued by NIST.

- IPSS Risk Assessment Report, August 14, 2003.
- IPSS System Security Plan, June 30, 2003, revised August 14, 2003.
- IPSS Contingency Plan, July 25, 2003.
- IPSS Security Test Plan, July 25, 2003.
- Certification Memorandum, October 1, 2003.
- Accreditation Memorandum, October 6, 2003.
- Privacy Impact Assessment.
- FY 2003 and draft FY 2004 IPSS 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 IPSS.

2 Purpose

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

[3] A system's life cycle typically comprises five phases: initiation, development/acquisition, implementation, operation/maintenance, and disposal. In the implementation phase, the system is installed, acceptance testing is performed, and users are trained.
[4] 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.
[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 IPSS security documentation and found that:

- The security test and evaluation conducted on the system was not comprehensive and was not independent.
- IPSS security documentation is not always consistent with NIST guidelines.
- Security protection requirements are inconsistent within IPSS security documentation.

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

3.1 Security Test and Evaluation Was Not Comprehensive and Was Not Independent

NIST Special Publication (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." However, the security test and evaluation conducted on IPSS was not comprehensive, the test results were not fully documented, and the testing was not performed by an independent party.

The IPSS Security Test Plan, dated July 25, 2003, describes the software development life cycle tests most commonly used in the industry. The document describes the procedures for problem resolution, including problem identification, problem recording, problem tracking, problem resolution, and regression testing. The document includes a requirements map of requirement numbers from the IPSS Design Document to the requirement area and a requirement description and relevant test scenario number. Each Test Scenario includes a Summary of Test Case Overview, objectives, test roles and test approach; step numbers; actions for the tester to execute; expected results; description of the user's actions required to test the system; requirement being tested (where applicable); pass/fail indication, including the method used to complete the test (I-inspection, A-analysis, D-demonstration, T-test), and tester comments. Each test scenario also includes a place to record the tester name, date tested, and any witnesses to the test.

OFFICIAL USE ONLY PARAGRAPH REDACTED FOR PUBLIC RELEASE

OFFICIAL USE ONLY PARAGRAPH REDACTED FOR PUBLIC RELEASE

(Paragraph continued from previous page) **OFFICIAL USE ONLY PARAGRAPH REDACTED FOR PUBLIC RELEASE**

The IPSS Security Test 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 final IPSS Security Test Plan (and Report) delivered to NRC was actually a copy of the draft IPSS Security Test Plan, with the handwritten notes from the testing, and with the word "Draft" crossed out and replaced with the word "FINAL" on the cover.

The contractor that developed the system performed the security test and evaluation. The IPSS Security Test Plan and Report stated that the assigned test personnel are not part of the product development staff, and therefore will be able to approach the testing from a non-biased perspective. However, none of the pages used to record the testing results contain the tester name, date tested, or witnesses to the test. Therefore, Carson Associates could not validate the independence of the personnel performing the testing. 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:

1. Re-certify and re-accredit IPSS based on an independent, comprehensive, and fully documented assessment of all management, operational, and technical controls.

3.2 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 developing 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 Governmentwide policies, standards, and procedures issued by OMB, 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 IPSS Risk Assessment Report, System Security Plan, and Contingency Plan and found that while the documentation is up-to-date, it is not always consistent with NIST guidelines.

IPSS Risk Assessment Report Is Not Consistent With NIST Guidelines

The IPSS Risk Assessment Report, dated August 14, 2003, follows the guidance in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. However, the Risk Assessment Report is not consistent with the referenced NIST document. Specifically, the Risk Assessment Report (1) contains several errors in the calculated risk levels, (2) does not include recommendations for low level risks, and (3) **OFFICIAL USE ONLY SENTENCE REDACTED FOR PUBLIC RELEASE** and (4) only identified risks that are potential in the IPSS environment.

The IPSS Risk Assessment Report uses a series of tables to present the risk assessment results. The following is a brief description of each of the tables.

- Table E.5-1, Vulnerability/Threat Pairs, presents vulnerability/threat pairs and includes columns for vulnerability, threat-source, and threat action.
- Table E.5-4, Likelihood Rating, presents the likelihood[10] for each vulnerability/threat pair.
- Table E.5-6, Magnitude of Impact, presents the magnitude of impact[11] for each vulnerability/threat pair.

[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.
[10] Likelihood is the probability that a potential vulnerability may be exploited within the make-up of the associated threat environment.

- Table E.5-9, Risk Level, presents the risk level for each vulnerability/threat pair. Risk level is based on a combination of the likelihood rating and magnitude of impact.
- Table E.5-10, Control Recommendations, presents recommendations to address the vulnerabilities.
- Table E.6-1, List of Recommended Security Control, summarizes the vulnerabilities identified previously, and lists just the vulnerability with the recommended security control.

The presentation of the risk assessment results in a series of tables rather than in one or two consolidated tables makes is difficult for the reader to understand how the results in the separate tables relate to one another. For example, Table E.5-9 presents the risk level for each identified vulnerability. As stated previously, risk is based on a combination of the likelihood rating and magnitude of impact. However, Table E.5-9 does not include the likelihood and impact levels used to calculate the risk, so the reader must go back to previous tables to verify the risk level was calculated correctly.

The presentation of the risk assessment results in a series of tables also contributed to errors in the following tables of the IPSS Risk Assessment Report.

- One entry in Table E.5-9 has an incorrect risk level. The likelihood for this vulnerability/threat pair was medium, and the impact low; therefore the risk level should be low. However, the table lists the risk level as medium.
- There are two vulnerability/threat pairs in Table E.5-10 with incorrect risk levels. Both have a risk level of medium, when they should have a risk level of low.
- Table E.6-1 is missing a vulnerability that was identified as medium risk.

The IPSS Risk Assessment Report 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.

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. The IPSS risk assessment used only questionnaires and interviews with personnel responsible for the system to identify technical and non-technical vulnerabilities, resulting in identification of generic technical and non-technical

[11] Impact is the adverse impact of a security event in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality.

risk controls. The risk assessment did not include system security testing to identify actual vulnerabilities to IPSS.

The IPSS Risk Assessment Report stated that the vulnerability/threat pairs are those that are potential to the IPSS environment, and that more implementation specific recommendations would be offered as part of the security plan. **OFFICIAL USE ONLY SENTENCE REDACTED FOR PUBLIC RELEASE.**

RECOMMENDATION

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

2. Update the IPSS Risk Assessment Report to include:

   - Tables with accurate risk levels and all identified vulnerability/threat pairs.
   - Recommendations for all identified risks, or provide a rationale for providing only recommended controls for high and medium level risks.
   - A complete risk assessment of actual threats and vulnerabilities to IPSS.

IPSS System Security Plan Is Not Consistent With Guidance in NIST SP 800-18

OMB A-130 states that security plans shall be consistent with guidance issued by NIST. NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, provides an outline for a security plan and provides guidance on the content of the various sections. The Final System Security Plan for IPSS, dated June 30, 2003, and revised August 14, 2003, deviates from the outline in NIST SP 800-18 in some places.

NIST SP 800-18 recommends including the physical location and address of the office or organization responsible for a system. Section 2.2, Responsible Organization, of the IPSS System Security Plan contains no contact information – just the name of the office responsible for IPSS. In addition, the IPSS System Security Plan does not list the full name of the organization owning the system, just Security Branch. Section 5.1.1 of the IPSS System Security Plan states that the system owner is the NRC, Personnel Security Section. This contradicts the statement regarding the system owner in Section 2.2.

NIST SP 800-18 also recommends including the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for the system. Section 2.2 of the IPSS System Security Plan describes the responsibilities of the System Manager (noted as the Program Manager's role in the IPSS System Security Plan), but does not identify who this person is. The contact information for that role is not found until Section 2.8, Information Contacts. Examples in NIST SP 800-18 include the full address for each information contact, however the IPSS System Security Plan only includes name, phone number, and e-mail address.

NIST SP 800-18 recommends that the assignment of security responsibility be located in the first section of the security plan. However, this information is not found in the IPSS System Security Plan until Section 5.1.1. NIST SP 800-18 also recommends including the name, title, and telephone number for the security manager (and the example include the full address as well), however Section 5.1.1 of the IPSS System Security Plan only describes who has overall responsibility for the security of the data. The contact information is located in Section 2.8. The section on assignment of security responsibility also states that overall security management controls of the IPSS reside with the NRC OCIO, however the IPSS System Security Plan does not include any contact information for the personnel within OCIO who have this responsibility.

RECOMMENDATION

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

3. Update the IPSS System Security Plan to include:

   - Complete contact information for the responsible organization.
   - Consistent identification of the system owner.
   - Complete contact information for personnel supporting the system, including the Program Manager, and other NRC organizations providing support.
   - Assignment of security responsibility in a section consistent with NIST guidance.
   - Complete contact information for personnel with security responsibilities, including other NRC organizations with security responsibilities for the system.

IPSS System Security Plan Does Not Describe All Security Controls Identified As In-Place

NIST SP 800-18 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 IPSS, dated June 30, 2003, and revised August 14, 2003, where controls were not described.

In order to identify what controls are currently in place for IPSS, Carson Associates reviewed and analyzed the IPSS self-assessment and the results of security test and evaluation (ST&E) performed during the certification and accreditation of IPSS.

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 a

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 IPSS self-assessment in order to identify controls in place for IPSS. Any controls marked at least at a Level 3 in the IPSS 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.

As a result of the review of the IPSS System Security Plan and self-assessment, Carson Associates identified several cases where the information in the IPSS System Security Plan and self-assessment is inconsistent. The following are some examples:

- NIST SP 800-18 recommends a section on planning for security in the life cycle in the discussion of management controls. The IPSS System Security Plan only describes what phase the system is in, but does not discuss how security was handled during the applicable life cycle phase. The FY 2003 self-assessment had controls for both the initialization and deployment/acquisition phase all marked at Level 5, but none of the controls were described in the IPSS System Security Plan.
- NIST SP 800-18 recommends a section on incident response capability in the discussion of operational controls. The IPSS System Security Plan does not include a section specifically discussing incident response. The existence of an incident response capability is alluded to in other sections of the IPSS System Security Plan. Based on Carson Associates' knowledge of the NRC information security program, incident response is a function of the OCIO. The IPSS System Security Plan should include a discussion of this security control, even if it is brief and refers the reader to other documents or personnel for more details.
- **OFFICIAL USE ONLY PARAGRAPH REDACTED FOR PUBLIC RELEASE**

- **OFFICIAL USE ONLY PARAGRAPH REDACTED FOR PUBLIC RELEASE**

RECOMMENDATIONS

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

4. Update the IPSS System Security Plan to include a section on planning for security in the life cycle and a section on incident response capability.

5. Update the IPSS System 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 Report, or in any test and evaluation on controls added since publication of that report.

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

IPSS Contingency Plan Is Not Consistent With NIST Guidelines

Carson Associates reviewed the IPSS Contingency Plan, dated July 25, 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 IPSS Contingency Plan for consistency with NIST guidelines and found that in some instances, the IPSS Contingency Plan is not consistent with NIST guidelines.

NIST SP 800-34 describes one section of a contingency plan as a Concept of Operations section. This section should provide additional details about the system, the contingency planning framework, and response, recovery, and resumption activities. NIST SP 800-34 recommends including a general description of the system covered in the contingency plan. The description should include the system architecture, location(s), and any other important technical considerations. A system architecture diagram, including security devices (e.g., firewalls, internal and external connections), is useful. The content for the system description can usually be gleaned from the System Security Plan. The IPSS Contingency Plan does not include any kind of system description for IPSS, only minimum hardware configurations and a list of system priorities.

NIST SP 800-34 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, e-mail addresses, and home addresses). However, the personnel contact information in the IPSS Contingency Plan is not complete and not up-to-date. In addition, the personnel contact information is included within the document and not in an appendix as recommended by NIST SP 800-34. Section 2.2 of the IPSS Contingency Plan mentions assigned backups for the two key positions identified for IPSS, but the document does not provide any information on these backups, not even a name. In addition, the person identified as the IPSS System Manager is no longer employed at NRC. Not having up-to-date contact information to reach the designated personnel may cause delays in the disaster recovery process.

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 contingency plan should include a section describing responsibilities, including the overall structure of contingency teams and 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. The IPSS Contingency Plan includes a list of contacts in Section 2.1, but the document does not describe the structure and membership of the contingency teams.

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.

Despite these requirements, the IPSS Contingency Plan includes only three broad recovery strategies and does not include specific technical details on how to implement these strategies or what steps are needed for testing system functionality after restoration from backup.

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 IPSS Contingency Plan does not contain 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:

7. Update the IPSS Contingency Plan to include:

    - A description of the system covered in the contingency plan. The description should include the system architecture, location(s), and any other important technical considerations. A system architecture diagram, including security devices (e.g., firewalls, internal and external connections), is useful.

- Complete and up-to-date contact information for all personnel, including backup personnel responsible for implementing the IPSS Contingency Plan.
- 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.
- More detailed steps for recovery actions and assign procedures to the appropriate recovery team(s).
- 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.

3.3 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.

FIPS 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.[12] 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.

The IPSS System Security Plan defines protection requirements for IPSS as follows:

- Confidentiality – High
- Integrity – High
- Availability – Medium

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

However, the FY 2003 IPSS self-assessment and FY 2004 draft IPSS self-assessment define protection requirements for IPSS as follows:

- Confidentiality – High
- Integrity – High
- Availability – High

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 systems, especially if the change is from a lower rating to a higher one. If the protection requirements have changed since the IPSS System Security Plan was finalized, then an explanation for the change should be noted on the IPSS self-assessment.

RECOMMENDATION

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

8. Update the IPSS System Security Plan and/or IPSS self-assessment to consistently define the protection requirements (confidentiality, integrity, availability).

[Page intentionally left blank]

4 Consolidated List of Recommendations

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

1. Re-certify and re-accredit IPSS based on an independent, comprehensive, and fully documented assessment of all management, operational, and technical controls.

2. Update the IPSS Risk Assessment Report to include:

   - Tables with accurate risk levels and all identified vulnerability/threat pairs.
   - Recommendations for all identified risks, or provide a rationale for providing only recommended controls for high and medium level risks.
   - A complete risk assessment of actual threats and vulnerabilities to IPSS.

3. Update the IPSS System Security Plan to include:

   - Complete contact information for the responsible organization.
   - Consistent identification of the system owner.
   - Complete contact information for personnel supporting the system, including the Program Manager, and other NRC organizations providing support.
   - Assignment of security responsibility in a section consistent with NIST guidance.
   - Complete contact information for personnel with security responsibilities, including other NRC organizations with security responsibilities for the system.

4. Update the IPSS System Security Plan to include a section on planning for security in the life cycle and a section on incident response capability.

5. Update the IPSS System 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 Report, or in any test and evaluation on controls added since publication of that report.

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

7. Update the IPSS Contingency Plan to include:

   - A description of the system covered in the contingency plan. The description should include the system architecture, location(s), and any other important technical considerations. A system architecture diagram, including security devices (e.g., firewalls, internal and external connections), is useful.

- Complete and up-to-date contact information for all personnel, including backup personnel responsible for implementing the IPSS Contingency Plan.
- 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.
- More detailed steps for recovery actions and assign procedures to the appropriate recovery team(s).
- 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.

8. Update the IPSS System Security Plan and/or IPSS self-assessment to consistently define the protection requirements (confidentiality, integrity, availability).

5 OIG Response to Agency Comments

On December 13, 2004, the Executive Director for Operations provided comments concerning the draft system evaluation report. None of the comments required modifications to the report.

SCOPE AND METHODOLOGY

To perform the IPSS system evaluation, Carson Associates reviewed the system's security documentation, including the System Security Plan, Risk Assessment Report, self-assessment, Contingency Plan, Security Test Plan, 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.

The work was conducted from June 2004 to November 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.