OFFICE OF THE INSPECTOR GENERAL

U.S. NUCLEAR REGULATORY COMMISSION

Office of the Inspector General
System Evaluation of
Listed Systems That Process
Safeguards and/or Classified Information

OIG-05-A-14 August 4, 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/

August 4, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: SYSTEM EVALUATION OF LISTED SYSTEMS THAT PROCESS SAFEGUARDS AND/OR CLASSIFIED INFORMATION (OIG-05-A-14)

Attached please find the Office of the Inspector General's report, *System Evaluation of Listed Systems That Process Safeguards and/or Classified Information.* Richard S. Carson Associates, Inc. conducted this evaluation on our behalf and determined that:

- The inventory of listed systems is inaccurate and information is inconsistent.
- Some listed systems lack required security plans.
- Some security controls are not implemented as required.

The weaknesses identified are not significant deficiencies or reportable conditions. During an exit conference on July 15, 2005, 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

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
William N. Outlaw, Acting 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 Reactor and Preparedness Programs, OEDO
Martin J. Virgilio, Deputy Executive Director for Materials, Research, State and Compliance Programs, OEDO
Jacqueline E. Silber, Deputy Executive Director for Information Services and Administration, and Chief Information Officer, OEDO
William M. Dean, Assistant for Operations, OEDO
Timothy F. Hagan, Director, Office of Administration
Michael R. Johnson, Director, Office of Enforcement
Edward T. Baker, Director, Office of Information Services
James F. McDermott, Acting 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 the Inspector General
System Evaluation of
Listed Systems That Process
Safeguards and/or Classified Information

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

July 29, 2005

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, which include (1) an independent evaluation of an agency's information security program and practices and (2) 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 FY 2005 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 listed systems that process safeguards[1] and/or classified[2] information.

Listed systems represent one of four[3] categories used by NRC to group the agency's systems on its master inventory of systems. A listed system is a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which is not a major application when viewed from an agency perspective. Most of the systems in this category process safeguards and/or classified information. Many of the listed systems processing safeguards and/or classified information are either standalone personal computers (PCs) or laptops. None of these systems are connected to the NRC local area network when processing safeguards and/or classified information.[4]

PURPOSE

The system evaluation objective was to test the effectiveness of NRC security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information.

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

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

[3] The other three categories are major application, general support system, and other.

[4] Systems used to process safeguards and/or classified information may be connected to the NRC local area network, but only if the removable hard drive containing the safeguards and/or classified data is removed from the PC/laptop, and replaced with a separate hard drive used for unclassified processing.

RESULTS IN BRIEF

Carson Associates reviewed the security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information and found that:

- The inventory of listed systems is inaccurate and information is inconsistent.
- Some listed systems lack required security plans.
- Some security controls are not implemented as required.

Inventory of Listed Systems Is Inaccurate and Information Is Inconsistent

NRC Management Directive (MD) 12.5, *NRC Automated Information Security Program*, assigns the NRC Chief Information Officer responsibility for developing and maintaining a master inventory of all agency systems, including listed systems. This inventory is maintained by the Office of Information Services (OIS). Regional administrators, office directors, and system sponsors/owners are responsible for ensuring that information systems sponsored by their offices are included in the agency's master inventory of all agency systems. They are required to work with the agency to update and revalidate the master inventory of systems on an annual basis.

Despite this requirement, the master inventory of listed systems is not accurate and information for listed systems that are composed of multiple components is not consistently reported. The agency lacks procedures for maintaining and updating the inventory of listed systems.

Some Listed Systems Lack Required Security Plans

MD 12.5 requires all listed systems to have an up-to-date, approved security plan before the system is put into operation. Office directors, regional administrators, and system sponsors/owners are responsible for developing the security plans. The Chief Information Officer is responsible for reviewing and approving the security plans. However, some listed systems lack required security plans because the agency has not implemented procedures to ensure that all listed systems have approved, up-to-date security plans prior to a system becoming operational. Also, there are no procedures for ensuring that system owners/sponsors respond to agency requests for security plan updates in a timely manner.

Some Security Controls Are Not Implemented As Required

MD 12.5 describes the security controls required for all NRC systems, including listed systems. The agency has developed a security template that must be used for listed systems that process safeguards and/or classified information. This template includes additional security controls beyond those found in MD 12.5. Despite these requirements, some security controls are not being implemented as required because the agency has no procedures in place for verifying that security controls described in a system's security plan are actually being implemented.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve the security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information. A consolidated list of recommendations appears on page 11 of this report.

AGENCY COMMENTS

The Office of the Inspector General (OIG) provided this report in draft to agency officials and discussed its content at an exit conference on July 15, 2005. We modified the report as we determined appropriate in response to our discussion. Agency officials generally agreed with the report's findings and recommendations and opted not to include formal comments.

[Page intentionally left blank]

ABBREVIATIONS AND ACRONYMS

FISMA	Federal Information Security Management Act
FY	Fiscal Year
ID	Identifier
ISSO	Information System Security Officer
LAN	Local Area Network
MD	Management Directive
NRC	Nuclear Regulatory Commission
OIG	Office of the Inspector General
OIS	Office of Information Services
PC	Personal Computer

[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, which included FISMA.[5] FISMA outlines the information security management requirements for agencies, which include (1) an independent evaluation of an agency's information security program and practices and (2) 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 FY 2005 FISMA independent evaluation of NRC's information technology security program, Carson Associates reviewed security controls for listed systems that process safeguards and/or classified information.

Listed Systems That Process Safeguards and/or Classified Information

Listed systems represent one of four categories used by NRC to group the agency's systems on its master inventory of systems. A listed system is a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which is not a major application when viewed from an agency perspective. Most of the systems in this category process safeguards and/or classified information. Many of the listed systems processing safeguards and/or classified information are either standalone PCs or laptops. None of these systems are connected to the NRC local area network when processing safeguards and/or classified information.

Of the 179 listed systems on the agency's master inventory, 140 process safeguards and/or classified information. Carson Associates selected 61 of the 140 listed systems that process safeguards and/or classified information for evaluation, and reviewed any security plans and supporting documentation on file. Carson Associates met with the points of contact for 17 of the 61 selected listed systems to verify that security controls described in the security plan are actually implemented.

2 Purpose

The system evaluation objective was to test the effectiveness of NRC security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information.

3 Findings

Carson Associates reviewed the security policies, procedures, practices, and controls for listed systems processing safeguards and/or classified information and found that:

[5] 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.

- The inventory of listed systems is inaccurate and information is inconsistent.
- Some listed systems lack required security plans.
- Some security controls are not implemented as required.

3.1 Inventory of Listed Systems Is Inaccurate and Information Is Inconsistent

MD 12.5 assigns the NRC Chief Information Officer[6] responsibility for developing and maintaining a master inventory of all agency systems, including listed systems. This inventory is maintained by OIS, and includes the following information:

- Office – the NRC office that owns or sponsors the system.
- System – the system's name, which for listed systems is most often the tag number of the PC or laptop.
- Hardware – the system's hardware (Laptop, PC, Server, local area network (LAN),[7] and Other).
- Primary information system security officer (ISSO) – the primary ISSO appointed for the system.
- Phone # – primary ISSO's phone number.
- Type of information processed – five columns used to indicate the type of information processed by the system (e.g., safeguards, confidential, secret, top secret, sensitive compartmented information). A system can process more than one type of information. If no column contains a check mark, the system does not process safeguards and/or classified information.
- Security Plan Date – date of the security plan on file with OIS.
- Security Plan Current Status – status of the security plan (Final-Approved, Sent for Revision, Returned, Overdue, and Draft).
- System Status – current status of the system (Active, Develop, Retired, and Unknown).
- New Plan Due – date the system owner must submit an updated plan.

MD 12.5 requires regional administrators, office directors, and system sponsors/owners to ensure that information systems sponsored by their offices are included in the agency's master inventory of all agency systems. They are required to work with the agency to update and revalidate the master inventory of systems on an annual basis.

Despite the agency requirement for maintaining a master inventory of all agency systems, the master inventory of listed systems is not accurate and information for listed systems that are composed of multiple components is not consistently reported.

[6] In January 2005, the Office of the Chief Information Officer was renamed Office of Information Services. The Chief Information Officer is responsible for oversight of the Office of Information Services.

[7] The LANs found on the inventory of listed systems are standalone networks, and are not connected to the NRC network or any other network.

Inventory of Listed Systems Is Inaccurate

The following are some examples of inaccuracies found in the inventory.

- **Errors in the types of information handled by listed systems.** The first inventory of listed systems provided to Carson Associates by the agency included check marks in the safeguards column for systems that do not handle safeguards information. Carson Associates identified these inaccuracies while trying to select which listed systems to evaluate. OIS staff were not aware of the inaccuracies until Carson Associates brought them to their attention, and a revised inventory of listed systems was then provided.

  However, there are at least three systems on the revised inventory that are still incorrectly categorized according to the type(s) of data they process. One system had a check mark in the safeguards column, but the system does not process safeguards information. One system had check marks in the safeguards, confidential, and secret columns, but it only processes safeguards information. The third system had no check marks indicating the types of information handled by the system, when in fact it handles confidential, secret, top secret, and sensitive compartmented information. Carson Associates reviewed an inventory report from the FY 2004 FISMA evaluation and found that report also contained similar errors.

- **Errors in security plan dates.** Of the 61 listed systems chosen for evaluation, Carson Associates identified 3 with approved security plans on file with a more recent date than the security plan date in the inventory. In addition, Carson Associates identified two listed systems with approved security plans on file, but the inventory indicated either no security plan date/status, or that the security plan was sent back for revisions.

- **Errors in system status.** Of the 61 listed systems chosen for evaluation, 3 had a status of "Active," when in fact the systems were retired. Carson Associates learned from the system owner of one of the retired systems that another listed system, not chosen for evaluation, had also been retired. Another system chosen for evaluation had a status of "Active," but the security plan on file had a note on the cover stating the system was retired and the owner was being contacted for disposal.[8]

- **Errors in system tag numbers.** Of the 61 listed systems chosen for evaluation, 3 had incorrect tag numbers. These systems had been "refreshed" in the past year, and therefore had new tag numbers.[9] The inventory still used the previous tag number as the system name, making it difficult to determine if the system being evaluated was the correct system.

The agency lacks procedures for maintaining and updating the inventory of listed systems. For example, there are no procedures for updating the system name (i.e., tag number) or system status. One system owner stated that when one of their systems was retired, OIS asked for a

[8] MD 12.5 states that removable storage media that contain classified or sensitive information should be sent to the Division of Facilities and Security for retention or destruction.

[9] When the systems were refreshed, the removable hard drives containing safeguards and/or classified information were retained by the system owner for re-use in the new systems.

memorandum requesting the change in status. According to the system owner, the memorandum should address the disposition of the system, including the information residing on the system, and a statement that the system is no longer being used at NRC. Carson Associates could not find the requirement for this type of memorandum in any current NRC policy, so it is not clear how, or if, this requirement is conveyed to the system sponsors/owners.

Information for Listed Systems Composed of Multiple Components Is Not Consistently Reported

Some of the listed systems on the inventory are composed of multiple components. In some cases, each component is listed as a separate system on the inventory. In other cases, the individual components are not listed as separate systems, but are represented as one system on the inventory. The following are examples of inconsistencies in how listed systems composed of multiple components are reported on the inventory.

- The inventory of listed systems includes 10 systems owned by the Office of the Chief Financial Officer. Of the 10, 9 systems are actually a group of applications that, along with the License Fee Reports System, compose the Fee Systems, which is a major application, not a listed system. The inventory of listed systems indicates these systems lack security plans, when in fact they are covered by the Fees Systems security plan and do not require separate security plans.
- Of the 61 listed systems selected for evaluation, 7 were listed with a hardware type of "Other." Two of the seven were actually printers associated with other listed systems on the inventory. None of the other listed systems selected for evaluation that have printers associated with them have their printers listed on the inventory.
- There are three listed systems on the inventory with a hardware type of "LAN." These are systems that are composed of several workstations, servers, and printers, yet they are represented on the inventory as a single system. However, Carson Associates identified five systems on the inventory that actually compose another standalone network. In this case, the components of the standalone network are listed individually on the inventory, instead of as a single system.

RECOMMENDATIONS

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

1. Correct the inaccuracies in the inventory of listed systems.
2. Validate the inventory of listed systems annually.
3. Develop procedures for notifying OIS of changes in system information for listed systems on the inventory.
4. Develop procedures for recording inventory information for listed systems that are composed of multiple components.

3.2 Some Listed Systems Lack Required Security Plans

MD 12.5 requires all listed systems to have an up-to-date, approved security plan before the system is put into operation. Office directors, regional administrators, and system sponsors/owners are responsible for developing the security plans. The Chief Information Officer is responsible for reviewing and approving security plans. Security plans prepared for listed systems that process safeguards and/or classified information are required to use the abbreviated security plan format that is provided by OIS.

The completed security plan is to be submitted to OIS with a memorandum that (1) documents how the security requirements to protect the sensitive information are being satisfied, (2) discusses the implemented security controls, and (3) describes any residual risks that may exist. The security plan is reviewed by OIS staff, and approval of the abbreviated security plan results in system security accreditation (which is the management approval to operate). Approval is indicated either by a memorandum from the Senior Information Technology Security Officer stating that the plan has been approved, or by a signature page attached to the plan with signatures from the system owner and the designated approving authority indicating the plan has been approved. If the system is maintained off-site, a signed agreement that governs this off-site arrangement must be attached to the security plan.

- **Missing security plans.** Of the 61 listed systems chosen for evaluation, 14 lack required security plans. Of the 14, 12 are "Active" systems. Of the 12 "Active" systems, 3 have no security plan on file, 2 have security plans that have been submitted to OIS, but they have been sent back to the system owner/sponsor for revisions, 2 have a security plan status of "Draft," and 5 have overdue security plans.
- **Approved security plans without supporting documentation.** Of the 61 listed systems chosen for evaluation, 2 had a status of "Final –Approved," but the agency did not have supporting documentation on file indicating the security plan was actually approved. Carson Associates also identified two more listed systems that have approved security plans, but the security plans are marked "Confidential" and are on file with the system owner instead of with OIS. However, the final memoranda approving the systems were not marked "Confidential," and were not on file with OIS. The system owner stated that they submitted the required documentation to OIS for one of the systems, however there is nothing on file indicating where that documentation can be located. Of the 61 listed systems chosen for evaluation, 2 are stored off-site (one in Baltimore, Maryland, and one in Chicago, Illinois), however, the required off-site storage agreement was not attached to their security plans.
- **Overdue security plans.** Of the 79 listed systems that process safeguards and/or classified information that Carson Associates did not select for evaluation, the inventory indicates that 66 of them are "Active." Yet, 2 have no security plans and 22 have security plans that have been sent back to the system owner/sponsor for revisions. Two were sent back over 6 months ago, 16 were sent back over a year ago, and 4 were sent back over 2 years ago. Of the 79 systems, 6 have a system status of "Develop" and also do not have approved security plans. The inventory indicates that the security plans for the development systems were also sent back for revisions over a year ago.

Some listed systems lack required security plans because the agency has not implemented procedures to ensure all listed systems have approved, up-to-date security plans in place prior to a system becoming operational. System owners/sponsors are operating listed systems without an approved security plan because the agency has no procedures for ensuring system owners/sponsors respond to OIS requests for security plans and security plan updates in a timely manner. The agency cannot be certain that system sponsors/owners of listed systems processing safeguards and/or classified information have adequate controls in place to protect the information because not all of the systems have the required security plans.

RECOMMENDATIONS

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

5. Develop procedures for ensuring all listed systems have an up-to-date, approved security plan prior to being put into operation.
6. Develop procedures for ensuring system owners/sponsors respond to OIS requests for security plan updates in a timely manner.

3.3 Some Security Controls Are Not Implemented As Required

MD 12.5 describes the security controls required for all NRC systems, including listed systems. Some of these security controls, as they apply specifically to systems that process safeguards and/or classified information, are derived from other NRC Management Directives and Federal regulations, including:

- NRC MD 12.1, *NRC Facility Security Program*
- NRC MD 12.2, *NRC Classified Information Security Program*
- NRC MD 12.3, *NRC Personnel Security Program*
- NRC MD 12.6, *NRC Sensitive Unclassified Information Security Program*
- Department of Defense 5220.22M, National Industrial Security Program Operating Manual (February 2001)
- National Telecommunication and Information Systems Security Advisory Memorandum on Office Automation Security Guideline (January 1987)

The agency has also developed a security plan template that must be used for listed systems that process safeguards and/or classified information. This template includes additional security controls beyond those found in MD 12.5. Listed systems that process safeguards and/or classified information are required to have the following controls in place.

- **Warning banner.** MD 12.5 requires NRC systems to be configured to display a warning banner to users upon first accessing NRC automated information resources. The security plan template does not specify the use of a warning banner.

- **Unique user identifiers (IDs).** MD 12.5 requires user IDs to be issued on a one-to-one basis, and group user IDs are not permitted without special authorization. The security plan template requires all personnel authorized to process data on the system to be assigned a unique account, user name, and password to access the system.
- **Password change.** MD 12.5 requires systems to automatically force all users to change passwords at specified time intervals. The security plan template does not require users to change passwords at specified time intervals.
- **Screen saver.** MD 12.5 requires a password protected screen saver, set to activate after 15 minutes of inactivity. The security plan template includes a stronger requirement for screen savers. The screen saver must activate after 5 minutes of inactivity.
- **Audit trails.** MD 12.5 describes auditing controls as security controls that support accountability by providing a chronology of user actions. They should be applied commensurate with the risks and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system or the information it processes. The security plan template requires that (1) each user's actions on the system are to be audited and (2) the audit logs are to be reviewed at least monthly.
- **Sensitivity marking.** MD 12.5 requires all media containing sensitive information to be clearly labeled to indicate the sensitivity level of the most sensitive information contained on the media. The sensitivity level of the data should be clearly visible in human readable form on its exterior, electronically within the file containing the sensitive information, and on workstation, console, and PC monitor screens whenever sensitive information is displayed. The security plan template includes a stronger requirement for sensitivity marking. The system must have a display background indicating the type of data being processed.
- **Configuration management.** The security plan template requires information technology security patches to be applied to the operating system and installed software. The frequency is not defined in the template.
- **Virus updates.** The security plan template requires virus signatures to be updated weekly.

Carson Associates met with the points of contact for 17 of the 61 selected listed systems to verify that security controls described in the respective security plans are actually implemented, and found that some security controls are not being implemented as required.

- **Warning banner.** Of the 17 systems evaluated, 7 do not display any type of warning banner prior to users accessing the system. Of these seven, three are systems running operating systems that do not support individual user IDs. Therefore, displaying a warning banner prior to user access is not possible.
- **Unique user IDs.** Of the 17 systems evaluated, 3 do not have separate accounts for each user authorized to use the system. These systems are running an operating system that does not support individual user IDs.

- **Password change.** At least 2 of the 17 systems evaluated do not force users to change their passwords at specified time intervals. Both of these systems are running operating systems that support the enforcement of periodic password changes.
- **Screen saver.** Of the 17 systems evaluated, 4 do not have any type of screen saver. One of these systems is running an operating system that does not support a screen saver, and the configuration of that system is controlled by another Federal agency that provides NRC with the software to run the system. Three additional systems have screen savers, but all three activate after more than 5 minutes of inactivity, as required in the security plan template. In addition, one of them is not password protected.
- **Audit trails.** Of the 17 systems evaluated, 3 do not audit user actions. Two additional systems audit user actions, but the audit trails are not reviewed as required.
- **Sensitivity marking.** Of the 17 systems evaluated, 5 do not have a background display indicating the type of information being processed as required by the security plan template. However three of them have external labels on the PC or laptop indicating the type of information being processed, as required by MD 12.5.
- **Configuration management.** Of the 17 systems evaluated, 5 have not had any security patches applied to their operating systems, despite the release of security patches for the operating systems after the systems were put into operation.
- **Virus updates.** Of the 17 systems evaluated, 3 have not updated their virus signatures as required. Virus signatures were updated on one of the three systems once after the system was put into operation, but they have not been updated since.

Security controls are not being implemented as required because the agency has no procedures in place for verifying that security controls described in a system's security plan are actually being implemented. In addition, some of the operating systems currently in use on the listed systems that were evaluated do not support some of the required security controls.

The Chief Information Officer may grant exceptions to or deviations from MD 12.5,[10] however none of the security plans indicated that the systems were granted exceptions for not implementing some of the required security controls. Therefore, Carson Associates could not determine whether the deviations from the required security controls were made with approval from the Chief Information Officer, or whether the security controls were just not being implemented.

Although the risk associated with the lack of security controls for listed systems that process safeguards and/or classified information is reduced since they are rarely, if ever, connected to a network, NRC is not in compliance with its requirements for implementing security controls on listed systems that process safeguards and/or classified information.

[10] Exceptions to or deviations from MD 12.5 may be granted except for those areas in which the responsibility or authority is vested solely with the Commission, the Executive Director for Operations, or the Office of Administration and is not delegable, or for matters specifically required by law, Executive order, or directive to be referred to other management officials.

RECOMMENDATIONS

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

7. Develop procedures for verifying all required security controls are implemented on listed systems.
8. Require listed systems that process safeguards and/or classified information to use operating systems that support the implementation of required security controls.
9. Require security plans to include documentation approving any exceptions to the required security controls.
10. Modify the security plan template for listed systems that process safeguards and/or classified information to require warning banners and password changes at specified time intervals.

[Page intentionally left blank]

4 Consolidated List of Recommendations

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

1. Correct the inaccuracies in the inventory of listed systems.
2. Validate the inventory of listed systems annually.
3. Develop procedures for notifying OIS of changes in system information for listed systems on the inventory.
4. Develop procedures for recording inventory information for listed systems that are composed of multiple components.
5. Develop procedures for ensuring all listed systems have an up-to-date, approved security plan prior to being put into operation.
6. Develop procedures for ensuring system owners/sponsors respond to OIS requests for security plan updates in a timely manner.
7. Develop procedures for verifying all required security controls are implemented on listed systems.
8. Require listed systems that process safeguards and/or classified information to use operating systems that support the implementation of required security controls.
9. Require security plans to include documentation approving any exceptions to the required security controls.
10. Modify the security plan template for listed systems that process safeguards and/or classified information to require warning banners and password changes at specified time intervals.

5 OIG Response to Agency Comments

OIG provided this report in draft to agency officials and discussed its content at an exit conference on July 15, 2005. We modified the report as we determined appropriate in response to our discussion. Agency officials generally agreed with the report's findings and recommendations and opted not to include formal comments.

SCOPE AND METHODOLOGY

To perform the system evaluation of listed systems that process safeguards and/or classified information, Carson Associates reviewed the agency's inventory of listed systems, and selected a subset of listed systems for evaluation. Only listed systems processing safeguards and/or classified information were selected. Carson Associates selected at least one system for each NRC office that processes safeguards and/or classified information, and reviewed the security plans and other documentation on file. Carson Associates met with the points of contact for some of the systems to verify that security controls described in the security plan are actually implemented. The inventory of listed systems was also evaluated for overall accuracy and compliance with NRC policies and procedures.

Of the 179 listed systems on the agency's master inventory, 140 process safeguards and/or classified information. Carson Associates selected 61 of the 140 listed systems that process safeguards and/or classified information for evaluation, and reviewed any security plans and supporting documentation on file. Carson Associates met with the points of contact for 17 of the 61 selected listed systems.

The work was conducted from April 2005 to June 2005 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.

[Page intentionally left blank]