EVALUATION REPORT

Evaluation of NRC's Automated Information System Inventory Process

OIG-05-A-22 September 30, 2005

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/

September 30, 2005

MEMORANDUM TO: Luis A. Reyes
Executive Director for Operations

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

SUBJECT: EVALUATION OF NRC'S AUTOMATED INFORMATION SYSTEM INVENTORY PROCESS (OIG-05-A-22)

Attached please find the Office of the Inspector General's report *Evaluation of NRC's Automated Information System Inventory Process.* Richard S. Carson and Associates, Inc., conducted this evaluation on our behalf and found that:

- Information in NRC automated information system (AIS) inventories is inaccurate and inconsistent.
- NRC AIS inventory systems are not designed to capture all of the data needed to meet Federal requirements.

During an exit conference on September 21, 2005, NRC officials provided comments concerning the draft audit report, generally agreeing with the report contents. Subsequently, the agency elected 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 andT 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
Guy P. Caputo, Director, Office of Investigations
Edward T. Baker, Director, Office of Information Services
James F. McDermott, 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
Evaluation of NRC's
Automated Information System Inventory Process

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

September 30, 2005

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

[Page intentionally left blank]

EXECUTIVE SUMMARY

BACKGROUND

On December 17, 2002, the President signed the E-Government Act of 2002, which included the Federal Information Security Management Act (FISMA) of 2002. FISMA outlines the information security management requirements for agencies, including the requirement to develop and maintain an inventory of major information systems operated by or under control of the agency. The inventory must include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency, and must be updated at least annually. The inventory shall also be used to support information resources management.

Management Directive (MD) and Handbook 12.5, *NRC Automated Information Security Program*, assigns the NRC Chief Information Officer (CIO) responsibility for developing and maintaining a master inventory of all agency systems. MD and Handbook 2.1, *Information Technology Architecture*, assigns the NRC CIO responsibility for developing, maintaining, and implementing the NRC Information Technology Architecture (ITA). The agency maintains two inventories, the Information Technology Systems Security Tracking System (ITSSTS) and the Enterprise Architecture Repository System (EARS), to meet the requirements outlined in MD and Handbooks 12.5 and 2.1, respectively.

PURPOSE

The objective of this review was to evaluate NRC's process for maintaining an inventory of automated information systems (AIS).

RESULTS IN BRIEF

Carson Associates evaluated NRC's AIS inventory process and found that:

- Information in NRC AIS inventories is inaccurate and inconsistent.
- NRC AIS inventory systems are not designed to capture all of the data needed to meet FISMA requirements.

Information in NRC AIS Inventories Is Inaccurate and Inconsistent

Despite the requirements outlined in MD and Handbooks 12.5 and 2.1 for maintaining AIS inventories, the information in NRC AIS inventories is inaccurate and inconsistent because the procedures for maintaining and updating AIS inventories are inadequate. The lack of adequate procedures not only results in the inaccurate and inconsistent data, but also results in duplicative efforts for NRC offices. As a result of inaccurate and inconsistent data in the AIS inventories, the agency lacks a complete understanding of what AISs are currently in use, and therefore cannot support two of the five areas of

information resources management specified by FISMA. Without knowing what information technology is in place, the agency cannot adequately plan, budget, acquire, and manage information. The agency also cannot adequately monitor, test, and evaluate security controls for AISs as required by FISMA.

NRC Automated Inventory Systems Are Not Designed to Capture All of the Data Needed to Meet FISMA Requirements

As stated previously, FISMA requires development of an inventory of major information systems that shall be used to support five areas of information resources management. However, neither ITSSTS nor EARS were designed to capture all of the data needed to fully meet these requirements. For example, only one inventory system captures the data needed to indicate which systems include Privacy Act data, and not all systems that include Privacy Act data are correctly identified. The agency cannot provide effective privacy protections, and cannot test and evaluate those protections, if it cannot identify which systems contain Privacy Act data. In addition, neither inventory system captures the data needed to support (1) preparation and maintenance of the inventory of information resources required to support the Government Information Locator Service, (2) preparation of the index of major information systems required under the Freedom of Information Act, and (3) preparation of information system inventories required for records management.

RECOMMENDATIONS

This report makes recommendations to the Executive Director for Operations to improve the NRC AIS inventory process. A consolidated list of recommendations appears on page 13 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 September 21, 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.

ABBREVIATIONS AND ACRONYMS

AIS	Automated Information System
Carson Associates	Richard S. Carson and Associates, Inc.
CIO	Chief Information Officer
EARS	Enterprise Architecture Repository System
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GSS	General Support System
ITA	Information Technology Architecture
ITIM	Information Technology Investment Management
ITSSTS	Information Technology Systems Security Tracking System
MA	Major Application
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSTS	National Source Tracking System
OIG	Office of the Inspector General
OIS	Office of Information Services
PASS	Property and Supply System
RPS	Reactor Program System
SP	Special Publication
U.S.C	United States Code

[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.[1] FISMA outlines the information security management requirements for agencies, including the requirement to develop and maintain an inventory of major information systems operated by or under the control of the agency. The inventory must include an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. The inventory is required to be updated at least annually. The inventory shall be used to support information resources management, including:

- Preparation and maintenance of the inventory of information resources required to support the Government Information Locator Service.[2]
- Information technology planning, budgeting, acquisition, and management.
- Monitoring, testing, and evaluation of information security controls.
- Preparation of the index of major information systems required under the Freedom of Information Act.
- Preparation of information system inventories required for records management.

NRC AIS Categories

NRC uses four categories to describe its AISs, as follows:

- Major Application (MA) – a computerized information system or application that requires special attention to security because of the risk and magnitude of harm that would result from the loss, misuse, or unauthorized access to or modification of the information in the application.
- General Support System (GSS) – an interconnected set of information resources under the same direct management control that share common functionality. Typical GSSs are local and wide area networks, servers, and data processing centers.
- Listed – 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 an MA or GSS when viewed from an agency perspective. Sensitive data may include individual Privacy Act[3] information, law

[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] The Government Information Locator Service identifies and describes information resources throughout the Federal Government. It also describes how the public can obtain the information (an information locator).

[3] The Privacy Act of 1974 (5 U.S.C. § 552a), As Amended, was enacted to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy resulting from the collection, maintenance, use, and disclosure of personal information. The Privacy Act safeguards confidentiality by limiting or restricting disclosure of personally identifiable records maintained by Federal agencies.

enforcement sensitive information, sensitive contractual and financial information, safeguards, and classified information.

- Other – an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC local area network/wide area network. The Office of Information Services (OIS) and the system sponsor must first jointly decide that the application is appropriately called a system and is to be included in the NRC master inventory of systems.

NRC AIS Inventories

MD and Handbook 12.5, *NRC Automated Information Security Program,* assigns the NRC CIO responsibility for developing and maintaining a master inventory of all agency systems. The identification of all major information systems in the inventory must include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency.

MD and Handbook 2.1, *Information Technology Architecture,* assigns the NRC CIO responsibility for developing, maintaining, and implementing the NRC ITA.[4] According to MD and Handbook 2.1, the ITA:

- Ensures the integration and interoperability of technology in the NRC information technology environment.
- Reduces agency costs for data entry and maintenance; information technology development, maintenance, and operation; and training and support.
- Increases productivity by improving the quality of information and ensuring users have easier access to information.

The NRC ITA is also intended to support other agency processes, such as information technology capital planning and investment control and information technology acquisitions. One of the eight[5] components of the ITA is a database of information technology systems, including databases used for change management, integration and retirement of legacy systems, and ITA compliance certification. The ITA database is used by NRC project managers and OIS technical staff to track the status of systems during their life cycles, plan system retirements, and report on systems.

Information Technology Systems Security Tracking System (ITSSTS)

ITSSTS was created to meet the requirements outlined in MD and Handbook 12.5 for developing and maintaining a master inventory of all agency systems. ITSSTS is used to track information

[4] An ITA is an integrated framework for evolving or maintaining existing information technology and acquiring new information technology to achieve the agency's strategic goals and information resources management goals (Title 40 U.S.C. § 11315(a)). The term enterprise architecture is also used to describe an agency's ITA.

[5] The other seven components are the Enterprise Model, Strategic Data Model, Consolidated Data Model, Physical Technology Architecture, Systems Development Life Cycle Methodology, Technical Reference Model, and Data Administration Reference Manual.

on each MA and GSS, including the publication dates of relevant security documentation such as risk assessments, security plans, contingency plans, security test and evaluation plans and reports, and certification and accreditation reports. ITSSTS is also used to track information on Listed and Other systems. ITSSTS includes information on NRC AISs that are under development, operational, and no longer in use. NRC AISs that do not meet the criteria of a system as defined in MD and Handbook 12.5 are not tracked in ITSSTS. The OIS Program Management, Policy Development, and Analysis Staff, Computer Security Team, maintains ITSSTS.

ITSSTS includes the following types of information for each system:

- Office – the NRC office that owns or sponsors the system.
- System ID/System Name – the system's identifier (usually an acronym) and name.
- Type – the system type (MA, GSS, L – Listed, O – Other, Sub – subsystem to another system, eG – Electronic Government System).
- System Status – current status of the system (Active, Inactive, Development, Retired, Transitioned, and Unknown).
- Comments – additional system information, typically a description of what the system does.

The ITSSTS inventory provided by the agency on July 7, 2005, includes 501 individual systems.

Enterprise Architecture Repository System (EARS)

EARS was created approximately 1 ½ years ago to meet the requirements outlined in MD and Handbook 2.1 and is one part of NRC's ITA. EARS includes information on NRC AISs that are under development, operational, and no longer in use. Systems in EARS may not meet the criteria for inclusion in ITSSTS. For example, a system may be tracked in EARS because of its relationship to the NRC ITA; however, it may not meet the criteria for an NRC AIS as defined in MD and Handbook 12.5. The OIS Business Process Improvement and Applications Division, Quality Assurance and Technology Branch, is responsible for the ITA database.

EARS includes the following types of information:

- Office – the NRC office that owns or sponsors the system.
- System Name/Full Name – the system's identifier (usually an acronym) and name.
- Description – additional system information.
- System ID – numeric identifier assigned to the system.
- Status – current status of the system (Initial Concept, Planning, Full Acquisition, Steady State, and Mixed Life Cycle) – this field is empty for almost all of the systems in EARS.

The EARS inventory provided by the agency on August 23, 2005 (dated August 17, 2005), includes 404 individual systems.

2 Purpose

The objective of this review was to evaluate NRC's process for maintaining an inventory of AISs.

3 Findings

Carson Associates evaluated NRC's AIS inventory process and found that:

- Information in NRC AIS inventories is inaccurate and inconsistent.
- NRC AIS inventory systems are not designed to capture all of the data needed to meet FISMA requirements.

3.1 Information in NRC AIS Inventories Is Inaccurate and Inconsistent

MD and Handbook 12.5 require 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.

MD and Handbook 2.1 assign the CIO responsibility for establishing an agencywide data administration program to promote data integrity and quality, including establishing data stewardship[6] standards and practices. Regional administrators and office directors are responsible for ensuring that office or regional business data are managed by office and regional data stewards in conformance with NRC data administration policies, procedures, and standards.

Despite the requirements outlined in MD and Handbooks 12.5 and 2.1 for maintaining AIS inventories, the information in NRC AIS inventories is inaccurate and inconsistent.

Inaccurate Information

The following are examples of inaccurate information found in ITSSTS and EARS.

- **Missing data.** Many of the fields in both inventories contain no data. In some instances, the only information is the system name, making it difficult to identify what the system is used for.
- **Systems not assigned to an office.** Both inventories include systems that are not assigned to an office. Lack of an assigned office makes it difficult to get updated information for that system. Carson Associates identified more than 30 systems that are not assigned to an office.

[6] A data steward is an individual charged with monitoring and ensuring the accuracy, timeliness, and compliance of a designated subset of NRC data with information technology standards.

- **Variations in system name.** Carson Associates identified at least five systems in the two inventories that seem to be the same system, but have slight variations in the system name. Since ITSSTS does not contain a system ID, it was difficult to determine whether the two systems are actually the same system.
- **Duplicate systems.** Both inventories contain multiple entries for what seem to be the same systems. However, due to the lack of detailed information on these systems in the inventories, Carson Associates could not determine if these entries represented duplicate systems. There are approximately 18 systems in the AIS inventories with more than one entry.
- **Errors in system status.** Carson Associates identified over 100 systems that are either retired, inactive, or were determined not to meet the criteria of a system. These systems have a status of "Active" in ITSSTS. Most of these systems have no value in the "status" field in EARS. In addition, EARS does not have a status value used to indicate a system is no longer in use. Carson Associates also identified six systems marked as "Retired" that, according to data provided by the system sponsor/owner, are still "Active."
- **Errors in system type in ITSSTS.** Carson Associates identified at least 35 systems in ITSSTS categorized as "Other" that should be categorized as "Listed." MD and Handbook 12.5 define a "Listed" system as a computerized information system or application that processes sensitive information requiring additional security protections. As noted previously, sensitive data may include individual Privacy Act information, law enforcement sensitive information, or sensitive contractual and financial information. Carson Associates identified 11 systems that the sponsoring office identified as containing sensitive data, and 1 system that the sponsoring office identified as a "Listed" system, but were categorized as "Other" in ITSSTS. Carson Associates also identified 26 systems that may be systems of record[7] or duplicate systems of record[8] that were categorized as "Other" in ITSSTS. A system of records (or duplicate system of records) contains information protected by the Privacy Act, and therefore, should be categorized as a "Listed" system.
- **System interfaces.** In response to an FY 2003 FISMA independent evaluation recommendation that the agency update the master inventory of systems, the agency tasked a contractor to identify the interfaces for all systems under maintenance. The results of this information collection were provided to the Enterprise Architecture group (OIS Business Process Improvement and Applications Division, Quality Assurance and Technology Branch) for input into the agency's ITA. Carson Associates reviewed the system interface information collected by the contractor and found that it did not reflect all interfaces for NRC MAs and GSSs. For example, the interface information did not include interfaces between the Human Resources Management System and other NRC AISs. Carson Associates also reviewed the interface information in EARS (ITSSTS does not include interface information) and found that the interface information in EARS does

[7] A system of records is a group of Privacy Act records under the control of NRC from which information is retrieved by the name of an individual or by an identifying number, symbol, or other identifier assigned to an individual.

[8] A group of records that are similar to records contained in an NRC system of records. It need not contain all of the records contained in the primary system.

not reflect the interface information gathered by the contractor in response to the FY 2003 FISMA independent evaluation, nor does it reflect all interfaces for NRC MAs and GSSs.

Inconsistent Information

The following are examples of inconsistent information found in ITSSTS and EARS.

- **Systems in EARS but not in ITSSTS.** Carson Associates identified 95 systems that were in EARS but were not in ITSSTS. These systems may not meet the criteria for a system as defined in MD and Handbook 12.5, and therefore would not be tracked in ITSSTS. However, due to the lack of detailed information on these systems, Carson Associates could not determine whether they should be tracked in ITSSTS.
- **Systems in ITSSTS but not in EARS.** Carson Associates identified 192 systems that were in ITSSTS but were not in EARS. Of the 192, 42 are for actual systems, 9 appear to be dummy or temporary entries, and 141 are for standalone personal computers and laptops used to process safeguards and/or classified information. Systems that meet the criteria for a system and are tracked in ITSSTS are the types of systems that should also be tracked in EARS. Standalone PCs and laptops that process safeguards and/or classified information, which are considered to be Listed systems and that are tracked in ITSSTS, may not need to be tracked in EARS as they are standalone systems and are not part of the NRC ITA.
- **Inconsistent reporting of systems composed of multiple components.** Some of the systems in ITSSTS are composed of multiple components. In some cases, each component is listed as a separate system on the inventory. For example:
    - Four subsystems of the Reactor Program System (RPS) are listed as individual systems in ITSSTS. However, not all RPS subsystems are listed. Carson Associates identified at least nine additional RPS subsystems that are not included in ITSSTS.
    - Five subsystems of the Operations Center Information Management System are listed as individual systems in ITSSTS.
    - Nine systems owned by the Office of the Chief Financial Officer are subsystems of the Fee Systems. However, they are reported as individual systems.

  EARS has no mechanism for indicating a system is a subsystem.
- **Inconsistent reporting of "Codes."** NRC uses computer codes to evaluate thermal-hydraulic conditions, fuel behavior, and reactor kinetics during various operating and postulated accident conditions. Results from applying the codes support decisionmaking for risk-informed activities, the review of licensees' codes and performance of audit calculations, and the resolution of other technical issues. One office director inquired about whether or not "Codes" should be included on the inventories. The office director stated that in a previous exercise updating the NRC Enterprise Model Applications Inventory, they were informed that "Codes" should not be included. However, some offices included "Codes" on their inventory, and some indicated they should be removed.

Procedures for Maintaining and Updating AIS Inventories Are Inadequate

Information in the NRC AIS inventories is inaccurate and inconsistent because the procedures for maintaining and updating AIS inventories are inadequate. Specifically, the agency (1) lacks procedures for updating AIS inventories with information collected from office directors, regional administrators, and system sponsors/owners; (2) provides insufficient guidance to office directors, regional administrators, and system sponsors/owners when requesting information for the AIS inventories; (3) lacks procedures for adding new systems to the AIS inventories; and (4) lacks procedures for updating information for systems already in the inventory. The lack of adequate procedures not only resulted in the inaccurate and inconsistent data, but also resulted in duplicative efforts for NRC offices.

Lack of Procedures for Updating AIS Inventories With Information Collected

The FY 2003 FISMA independent evaluation recommended that the agency update the master inventory of systems. To address this recommendation, the agency issued a ticket to all NRC headquarters and regional offices to update their system inventory. This update request was combined with a request for input on the cost for internal use software, in part to minimize the impact on offices for duplicate data calls. The agency issued a memorandum on November 25, 2003, describing the data call and stating that in the future, the agency would be issuing two data calls per year to update/validate the data. The agency made subsequent data calls September 17, 2004, and June 3, 2005.

Carson Associates reviewed the data collected during the three data calls and found that neither EARS nor ITSSTS was updated with the data collected. For example, one office noted in its response to the 2004 data call that none of the updates provided in response to the previous year's request were applied. Another office noted in response to the 2005 data call that three of the systems assigned to their office had been transferred to another office in 1993, and that "it would seem that after 12 years they should no longer show up" on our list. It should also be noted that the agency is not meeting its commitment to conduct biannual data calls. Since the first data call in November 2003, the agency has only issued two more.

While the agency has implemented procedures to gather the information required for the inventories, it has not developed procedures for making sure the information is actually entered into the inventories. As a result, the inventories are not being updated annually as required by FISMA.

Insufficient Guidance Provided on Information Required

For the 2003 data call, each office was provided with a single-page "validation report" for each system sponsored by that office. A sample of the 2003 validation report can be found in Appendix B. For the 2005 data call, each office was provided with a three-page validation report. A sample of the 2005 validation report can be found in Appendix C. The offices were provided little or no guidance on the information being requested. The following are examples of the insufficient guidance provided to office directors, regional administrators, and system sponsors/owners when requesting information for the AIS inventories.

- The 2003 data call asked for the "A-130 Type," [9] and whether the system is one of the following: MA, GSS, Listed, or Other. However, the 2003 data call provided no guidance as to what A-130 Type means, what choices are valid for A-130 Type, and what the relationship is between A-130 Type and the other information system types. The 2003 data call also provided no guidance on the implications of indicating "Yes" for sensitive. According to MD and Handbook 12.5, if a system contains sensitive data, then the system is considered a "Listed" system.
- One office director responded to the 2003 data call with several questions pertaining to the data call, including:
    - Which fields need to be updated/completed (many of the fields do not apply to most systems)?
    - What are the choices for the A-130 field (what does Other and Non-Tracked System mean)?
    - Which systems need "Approval to Operate?"
    - Can you define "system" as far as what you want us to provide data?
- One office responded to the 2004 data call with a question about systems on their inventory that were actually subsets of a bigger system. The office asked for guidance on how those "subsystems" should be reported. As noted earlier, Carson Associates found several subsystems on the inventory, indicating that not enough guidance was provided on how these subsystems should be reported.
- The 2005 data call provided some guidance on the four system security categories found on the validation report by providing a reference to MD and Handbook 12.5. However, the 2005 data call did not provide any additional guidance, despite previous requests for clarification on the information requested.
- All three data calls request a list of interfacing systems, by System ID. However, the data calls did not provide the entire list of NRC AISs and their System IDs. In addition, the language used in the validation reports implies that only interfaces with other NRC AISs need to be reported. FISMA and MD and Handbook 12.5 require all interfaces to be included in the inventory, including interfaces with systems or networks not operated by or under the control of the agency.

Lack of Procedures for Adding New Systems

The agency lacks procedures for adding new systems to the AIS inventories. For example, EARS contains an entry for the National Source Tracking System (NSTS), a new system currently under development. The agency was made aware of this system during the 2004 data call, yet it was not included in the ITSSTS inventory provided to Carson Associates in July 2005. Carson Associates has subsequently learned that the NSTS is considered to be a Major Application, and should be tracked in ITSSTS. Due to the lack of procedures for adding new

[9] Carson Associates assumes that A-130 refers to OMB Circular A-130, *Management of Federal Resources*, which establishes policy for the management of Federal information resources.

systems to the AIS inventories, NSTS was omitted from ITSSTS. Another system Carson Associates identified in EARS but did not find in ITSSTS is EARS itself. EARS meets the criteria of a system as defined in MD and Handbook 12.5, yet it was never added to ITSSTS as a system.

Lack of Procedures for Updating Information for Existing Systems

The agency also lacks procedures for updating information for systems already in the inventories, other than through the biannual data calls. As a result, systems that are no longer being used are still being reported as "Active." Since the agency is currently issuing data calls only annually, inactive systems could remain on the AIS inventories as "Active" for at least a year. For example, one office reported in its response to the 2005 data call that three of its systems were not year-2000 compatible and their use was discontinued at the end of 1999. However, since the agency lacks procedures for offices to follow when a system retires or is no longer used, these systems were still being reported as active systems in the AIS inventories.

AIS Inventories Cannot Support Intended Functions

As stated previously, FISMA requires development of an inventory of major information systems that shall be used to support five areas of information resources management. However, as a result of inaccurate and inconsistent data in the AIS inventories, the agency lacks a complete understanding of what AISs are currently in use, and therefore cannot support two of the five areas of information resources management specified by FISMA. Without knowing what information technology is in place, the agency cannot adequately plan, budget, acquire, and manage information technology. The agency also cannot adequately monitor, test, and evaluate security controls for AISs as required by FISMA.

AIS Inventories Cannot Support Information Technology Planning, Budgeting, Acquisition, and Management

FISMA specifies the inventory shall be used to support information technology planning, budgeting, acquisition, and management under section 3506(h) of title 44, title III of title 40, and related laws and guidance. These statutes require agencies to design and implement a process for maximizing the value, and assessing and managing the risks, of agency information technology acquisitions. Agency programs supporting these statutes include the capital planning and investment control process and the agency ITA.

An important aspect of the capital planning and investment control process is the integration of information technology security. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*, dated January 2005, provides a systematic approach to selecting, managing, and evaluating information technology security investments. NIST SP 800-65 describes the creation of a system inventory as a key aspect of Stage Two (building the investment foundation) of the Information Technology Investment Management (ITIM) maturity framework.[10] The

[10] The ITIM maturity framework is a five-stage model, developed by the Government Accountability Office, for assessing the maturing of agencies' investment management practices.

system inventory ensures the agency can identify cost, benefit, schedule, risk, and investment ownership information and review investment performance accordingly.

NIST SP 800-65 further states that both FISMA and the ITIM framework require the development of a system inventory. The system inventory is a cornerstone of the ITIM framework and also relates directly to investment security concerns. NIST recommends that agencies work to build a single system inventory that meets the requirements of both the ITIM framework and FISMA.

MD and Handbook 2.1 include an exhibit that shows how each ITA component is used during the applications system life cycle. The ITA database is intended to support the following life cycle phases:

- Planning – to see if a system already exists; plan for integration and retirement.
- Acquisition –to ensure acquisitions integrate with existing systems.
- Development – to track the status of developing new systems.
- Operations and Maintenance – to track and report on current systems.
- Decommissioning – to plan system retirements.

However, neither ITSSTS nor EARS can be used to support information technology planning, budgeting, acquisition, and management as described in Federal statutes and MD and Handbook 2.1, because both inventories contain inaccurate data. For example, the first step in planning a new information technology acquisition is to determine whether the agency already has a system that provides the functions sought from the new system. This step cannot be performed if the agency does not have an accurate inventory of systems already in use, including specifics on what functions those systems provide.

AIS Inventories Cannot Support Monitoring, Testing, and Evaluation of Information Security Controls

FISMA also states the inventory shall be used to support monitoring, testing, and evaluating information security controls. FISMA requires agencies to periodically test and evaluate information security controls and techniques for the information and information systems that support the agency to ensure that they are effectively implemented. This requirement includes testing of management, operational, and technical controls of every information system identified in the inventory required by FISMA. MD and Handbook 12.5 define the security controls required for each of the four categories of AISs. However, the agency cannot monitor, text, and evaluation information security controls if it does not have an accurate inventory of systems in use.

RECOMMENDATIONS

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

1. Correct the inaccuracies in the AIS inventories.

2. Validate the information in the AIS inventories annually.
3. Provide guidance on the type of information required from the office directors, regional administrators, and system owners/sponsors when providing AIS inventory updates.
4. Develop and implement procedures for adding new systems to the AIS inventories.
5. Develop and implement procedures for notifying OIS of changes in system information in the AIS inventories.
6. Develop and implement procedures for recording system information for systems that are composed of multiple components.

3.2 NRC AIS Inventory Systems Are Not Designed To Capture All of the Data Needed To Meet FISMA Requirements

As stated previously, FISMA requires development of an inventory of major information systems that shall be used to support five areas of information resources management. However, neither ITSSTS nor EARS were designed to capture all of the data needed to fully meet these requirements. Specifically:

- Only one inventory system captures the data needed to indicate which systems include Privacy Act data.
- Neither inventory system captures the data needed to support other information resources management functions required by FISMA.

As a result, NRC AIS inventory systems do not meet FISMA requirements.

Only One Inventory System Indicates Which Systems Include Privacy Act Data

MD and Handbook 12.5 state that effective privacy protections are essential to all NRC AISs, especially those that contain substantial amounts of personally identifiable information. The use of new information technologies should sustain, and not erode, the privacy protections provided in all statutes and policies relating to the collection, use, and disclosure of personal information. However, only one inventory system captures the data needed to indicate which systems include Privacy Act data, i.e., which systems are electronic systems of records and which systems are duplicate systems of records. In addition, not all systems that include Privacy Act data are correctly identified in that inventory system. The agency cannot provide effective privacy protections, and cannot test and evaluate those protections, if it cannot identify which systems contain Privacy Act data.

Other Information Resources Management Functions

In addition to (1) information technology planning, budgeting, acquisition, and management and (2) monitoring, testing and evaluation of information security controls, FISMA identifies three other information resources management areas that shall be supported by the inventory:

- Preparation and maintenance of the inventory of information resources required to support the Government Information Locator Service.
- Preparation of the index of major information systems required under the Freedom of Information Act.
- Preparation of information system inventories required for records management.

Neither EARS not ITSSTS captures the data needed to support these areas of information resources management. For example, neither inventory system captures the data necessary to identify an AIS as an electronic records system.[11]

RECOMMENDATION

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

7. Modify the AIS inventory systems to capture all of the data needed to meet FISMA requirements.

[11] An electronic records system is any information system that produces, manipulates, or stores Federal records by use of a computer.

4 Consolidated List of Recommendations

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

1. Correct the inaccuracies in the AIS inventories.
2. Validate the information in the AIS inventories annually.
3. Provide guidance on the type of information required from the office directors, regional administrators, and system owners/sponsors when providing AIS inventory updates.
4. Develop and implement procedures for adding new systems to the AIS inventories.
5. Develop and implement procedures for notifying OIS of changes in system information in the AIS inventories.
6. Develop and implement procedures for recording system information for systems that are composed of multiple components.
7. Modify the AIS inventory systems to capture all of the data needed to meet FISMA requirements.

5 OIG Response to Agency Comments

OIG provided this report in draft to agency officials and discussed its content at an exit conference on September 21, 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

The scope of this report only includes inventories, and the systems used to maintain them, that the agency uses to track information about NRC AISs. This report does not address other types of inventories maintained by the agency or inventory systems used at the agency. For example, the Division of Administrative Services within the Office of Administration manages the Property and Supply System (PASS), which accounts for non-capitalized equipment.[12] While PASS may include information about the information technology equipment, such as servers, used to support NRC AISs, it does not include information about the AISs themselves. Therefore, PASS was not included within the scope of this evaluation.

To perform the evaluation of NRC's AIS inventory process, Carson Associates met with OIS staff responsible for maintaining ITSSTS and EARS. Carson Associates also compared the data in ITSSTS and EARS, based on inventories provided by the agency.

The work was conducted from July 2005 to August 2005 in accordance with guidelines from the National Institute of Standards and Technology, and best practices for evaluating security controls. Jane Laroussi, CISSP, from Carson Associates conducted the work.

[12] Non-capitalized equipment represents NRC property (either in the agency's possession or contractor-held) with an initial acquisition cost of less than $50,000. This includes information technology equipment.

[Page intentionally left blank]

All Systems Validation Report - ITSSTS

Organization:

System:

PDB Number:		*Mai*	*Ap*	*G S S*	*Listed*	*Other*	*Sensitive?*
A-130 Type							*Approval to Operate?*
POC:		*POC Phone:*					*POC E-Mail:*
ISSOs:		*Appointed:*					*ISSO Course Completion:*

	Development Cost	*Enhancement Cost*	*Total*	*Enhancements Completed or in Progress?*	*Yes* ___ *No* ___
Current Period:	_____	_____	_____	*Currently Operational?*	*Yes* ___ *No* ___
Total-to-Date:	_____	_____	_____		

Interfacing Systems (by PDB Number): _____ _____ _____ _____ _____

Required Documents:	*Status*	*Dated*
Risk Assessment		
System Security Plan		
Security Test and Evaluation		
Business Continuity Plan Test Report		
Certification Report		
Accreditation		

Comments:

Wednesday, November 12, 2003 8:30:08

[Page intentionally left blank]

All Systems Validation Report

Organization:

System:

System ID: **A-130 System Category:** **Major** ☐ **GSS** ☐ **Non-Tracked** ☐ **System Security Category:** **Major** ☐ **Listed** ☐ **GSS** ☐ **Other** ☐	**Currently Operational:** ☐ **Decommission Date:** _____ **Planned Decommission Date:** _____	**System contains sensitive data:** ☐ **System has an Approval to Operate:** ☐ **Date of approval:** _____

POC: **POC Phone:** **POC Email:**

ISSOs: **Date Appointed:** **ISSO Course Completion Date:**

	Development Cost	Enhancement Cost	Total	Enhancements Completed or in Progress:
Current Fiscal Year:	_____	_____		☐
Total-to-Date:	_____	_____	_____	

Interfacing Systems (by System ID): _____ _____ _____ _____

Required Documents:	**Status:**	**Dated:**
Risk Assessment:		
System Security Plan:		
Security Test and Evaluation:		
Business Continuity Plan Test Report:		
Certification Report:		
Accreditation:		

All Systems Validation Report

Organization:

System:

Comments:

System Software List: (Attach additional sheets if necessary.)

Software	**Version**

All Systems Validation Report

Organization:

System:

Server name/number and location where server resides: (Attach additional sheets if necessary.)

/24/2005

[Page intentionally left blank]