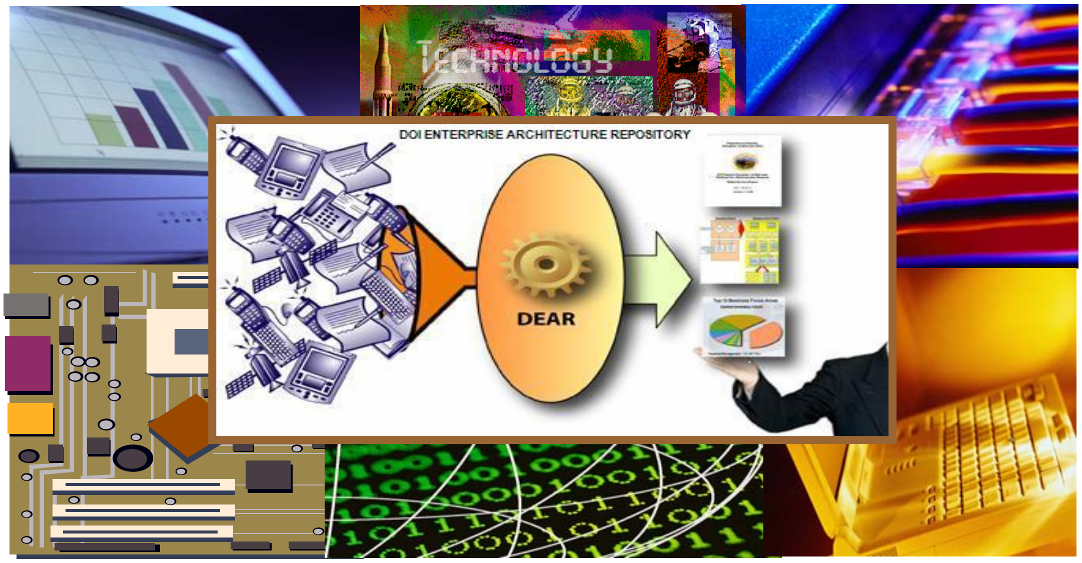
U.S. Department of the Interior
Office of Inspector General

Report No. C-EV-MOA-0003-2006



Department of the Interior
Information Technology (IT) Systems Inventory

EVALUATION REPORT

AUGUST 2006

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Central Region
134 Union Blvd., Suite 510
Lakewood, Colorado 80228

August 30, 2006

Memorandum

To: W. Hord Tipton
Chief Information Officer

From: Jack Rouch
Regional Audit Manager
Central Region

Subject: Final Evaluation Report, "Department of the Interior, Information Technology (IT) Systems Inventory" (No. C-EV-MOA-0003-2006)

The attached final report presents the results of our evaluation to determine whether the Department of the Interior (Department) has an adequate process for inventorying its IT systems. We concluded that the Department does have an inventory of its IT systems, but it needs to improve its internal controls relating to the IT systems inventory, require the bureaus to regularly review and certify the accuracy of their IT systems data in the inventory, and ensure that all systems in the inventory are properly mapped to an accreditation boundary.

Because this is a final report, a response to the recommendations from you to the Office of Inspector General is not required. We are referring the four recommendations in this report to the Department's Focus Leader for Management Control and Audit Follow-up for resolution and tracking of implementation.

The legislation, as amended, creating the Office of Inspector General requires that we report to Congress semiannually on all reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented. Consequently, we will include information from this report in our next semiannual report.

If you have any questions regarding this report, please call me at (303) 236-9243.

Attachment

EXECUTIVE SUMMARY

WHY WE DID THIS EVALUATION

The Federal Information Security Management Act (FISMA) requires adequate security measures and controls to be in place to protect IT systems and mission-critical data. To accomplish this, a complete and accurate IT systems inventory is essential.

Our FY2005 annual evaluation of DOI's information security program found that the use of multiple inventories resulted in discrepancies, making it difficult to maintain an accurate count of systems. Additionally, the process relied on manual efforts to reconcile the differences between the various inventories.

Our evaluation objective was to determine whether DOI has an adequate process for inventorying its IT systems.

We found that the Department of the Interior (DOI) has made significant progress in addressing our concerns about information technology (IT) systems inventory expressed in our report *Annual Evaluation of the Department's Information Security Program* (NSM-EV-MOI-0013-2005). The Office of the Chief Information Officer (OCIO) has initiated the consolidation of three separate IT systems inventories into its DOI Enterprise Architecture Repository (DEAR). Once completed, this consolidation should reduce discrepancies between multiple inventories and eliminate the need for time consuming manual reconciliations.

While OCIO has made progress in addressing our concerns with its IT systems inventory, we found four areas where controls could be strengthened by:

- ➢ establishing greater accountability for bureau Chief Information Officers (CIO) by requiring that they review and certify the completeness and accuracy of their IT systems inventories on an annual basis,
- ➢ mandating consistent DOI-wide procedures for maintaining the IT systems inventory or requiring bureau CIOs to document their individual procedures for implementing OCIO's general policies,
- ➢ documenting OCIO oversight procedures for the IT systems inventory process, and
- ➢ ensuring that all IT systems in DEAR are correctly mapped to an appropriate accreditation boundary.

We made four recommendations to help DOI improve its IT systems inventory process.

CONTENTS

INTRODUCTION

EVALUATION OBJECTIVE

This report presents the results of our evaluation of the Department of the Interior's (DOI) process for inventorying its information technology (IT) systems. Our objective was to determine whether DOI has an adequate process for inventorying its IT systems.

BACKGROUND

Legislation and guidelines have been enacted in recent years to help ensure the effectiveness of information security controls and to aid in achieving more secure IT systems within the federal government. For DOI to ensure that it has adequate security controls in place to protect its IT systems and mission-critical data, it must have an accurate and complete IT systems inventory.

The Federal Information Security Management Act of 2002 (FISMA) requires federal agencies to provide information security protections to prevent unauthorized access, use, disclosure, disruption, modification, or destruction of IT systems and data. FISMA also requires agencies to develop and maintain an inventory of major IT systems and to update the inventory annually.

The National Institute of Standards and Technology has established guidance requiring federal agencies to certify and accredit their systems. Certification requires a comprehensive assessment of security controls to ensure they are implemented correctly, operating as intended, and producing the desired outcomes. Accreditation refers to the agency's official management decision to authorize operation of an information system based on the implementation of security controls.

Historically, DOI has maintained three separate IT systems inventories:

1. DOI-wide inventory: The DOI-wide inventory has been maintained in a module of the DOI Enterprise Architecture Repository (DEAR) maintained by the Office of Chief Information Officer (OCIO).

2. Bureau-level inventories: Each DOI bureau has used a localized version of DEAR known as the Bureau Enterprise Architecture Repository (BEAR) to manage its separate IT systems inventories.

3. Certified and accredited systems inventory: DOI also maintained a separate inventory of IT systems that were certified and accredited in the DOI Command Center system.

DOI's primary guidance to ensure that it has an accurate and complete inventory is *OCIO Directive 2004-010*, dated April 2004. This policy stipulates that:

- All DOI systems and information technology investments will be tracked in DEAR.
- Bureau CIOs are responsible for ensuring the accuracy and completeness of their respective IT systems inventory and investments.
- The data in each system will be periodically updated.
- Any system that does not fall into the DOI-tracked system categories must still be tracked in the appropriate BEAR.
- For systems used by multiple bureaus, the bureau or office that manages the system is responsible for providing and updating information about it.

In our report, *Annual Evaluation of the Department's Information Security Program* (NSM-EV-MOI-0013-2005, dated October 2005), we expressed concerns about the use of multiple inventories and the discrepancies between those inventories. Using multiple inventories for reporting purposes makes it difficult to maintain an accurate inventory count. Additionally, we reported that the inventory process was not efficient because it relied on manual efforts to reconcile the various systems.

This report follows up on our previous concerns. Throughout this report, we note where OCIO has made progress in its IT systems inventory process and where additional improvements should be made. Appendix 1 contains information on the scope and methodology we used in conducting this evaluation. Appendix 2 provides additional information on related reviews.

EVALUATION RESULTS

OCIO HAS MADE SIGNIFICANT IMPROVEMENTS

We found that DOI has made progress in addressing the concerns about IT systems inventory that we expressed in our report *Annual Evaluation of the Department's Information Security Program* (NSM-EV-MOI-0013-2005).

DOI has initiated processes to consolidate the different IT systems inventories into DEAR. In April 2006, OCIO moved the inventory of certified and accredited systems from the DOI Command Center system to DEAR. OCIO is currently in the process of enabling bureaus to maintain their IT systems inventories directly in DEAR via real-time web access. This change, expected to occur this year, will eliminate the need to maintain separate inventories in DEAR and bureau BEARs. It will also eliminate the delay between when a system is entered by the bureau and when it actually appears in DEAR. Previously, bureaus input their systems information into their BEARs and then the data were merged into the DEAR during a quarterly synchronization process. These steps should help reduce discrepancies between multiple inventory systems and eliminate the need for time-consuming manual reconciliations.

INVENTORY CONTROLS CAN BE STRENGTHENED IN FOUR AREAS

While OCIO has taken significant steps to address problems with its IT systems inventory, we identified four areas where the controls could be strengthened to provide greater assurance of an accurate and complete DOI-wide inventory. These areas include:

- establishing greater accountability for bureau CIOs,
- documenting procedures for maintaining the IT systems inventory,
- documenting OCIO oversight of the IT systems inventory process, and
- ensuring that all IT systems in DEAR are correctly mapped to an appropriate accreditation boundary.

Establishing Greater Accountability for Bureau CIOs

The DOI CIO is ultimately responsible for completeness and accuracy of the DOI-wide IT systems inventory, which contained over 750 systems as of February 2006. However, OCIO must rely on the bureau CIOs to ensure that their IT systems inventory data are complete and accurate in their respective BEARs before the quarterly synchronization process occurs to update DEAR. In the future, OCIO will rely on bureau CIOs to ensure that their bureaus input complete and accurate IT systems inventory data directly into DEAR in a timely manner.

Despite OCIO's reliance on bureau CIOs, there is no requirement for them to periodically certify the completeness and accuracy of their inventory data. As part of our evaluation, we provided DEAR inventory listings to the Bureau of Land Management (BLM), the National Park Service (NPS), and the U.S. Geological Survey (USGS) and asked that they verify the completeness and accuracy of the inventory data. The NPS CIO's enterprise architect was unable to verify the completeness and accuracy of NPS' IT systems inventory data and stated that the DEAR data needed to be validated. After our site visit, the NPS enterprise architect provided OCIO a certification indicating that all major applications within NPS were included in the inventory and, to the best of his knowledge and belief, all other NPS systems were reflected in the inventory. The certification acknowledged that ongoing validation activities were underway to improve the quality of information related to the inventory.

In our opinion the process could be strengthened by OCIO requiring bureau CIOs to certify the completeness and accuracy of the DEAR inventory data on an annual basis in conjunction with FISMA's requirement for annual maintenance and update. This requirement would establish greater accountability for the bureau CIOs and should improve the reliability of the IT systems inventory data.

Establishing Procedures for Maintaining IT Systems Inventory

In September 2003, the Government Accountability Office (GAO) issued a report on BLM's management of its IT investments titled *Bureau of Land Management: Plan Needed to Sustain Progress in Establishing IT Investment Management Capabilities* (GAO-03-1025). In that report, GAO identified the following as a key practice:

> The organization has written policies and procedures for identifying its IT projects and systems and collecting, in an inventory, information about the IT projects and systems that is relevant to the investment management process.

The report concluded that BLM had not fully executed this key practice because it had not yet defined its policies and procedures for investment management purposes.

Our evaluation found that while *OCIO Directive 2004-010* established the general policy for the maintenance of an IT systems inventory, neither OCIO nor the bureaus have established procedures that document the steps used to implement the directive's requirements. In practice, we found that the three bureaus we visited established different approaches to maintaining their inventories. However, none of these approaches were formally documented in the form of written policies and procedures.

In our opinion, the inventory process would be strengthened by the establishment of DOI-wide procedures for inventory maintenance. However, at a minimum, OCIO should require bureau CIOs to document their individual procedures.

Documenting OCIO's Oversight Procedures

Our evaluation found that OCIO has not documented its procedures for providing oversight to the inventory process. To its credit, OCIO uses a number of procedures to help ensure a complete and accurate inventory.

- OCIO compares the DEAR inventory to annual Exhibit 300s used to report systems investments to the Office of Management and Budget.
- OCIO uses information from modernization blueprint projects to discover existing systems not included on the inventory. These projects include research to ascertain and document the current as-is system architecture business lines under review.
- OCIO reviews annual budget submissions to find any IT systems not identified in the current inventory.

However, none of these procedures have been formally documented. Documented procedures are important for establishing requirements, identifying responsible parties, describing actual steps for performing procedures, providing a basis for holding staff accountable for performing required procedures, and ensuring continuity of operations after staff turnover.

One additional area that needs to be documented is OCIO's procedures to provide oversight for new additions to the IT systems inventory. This is the ideal time for OCIO to provide oversight and ensure that bureaus are inputting complete and accurate data for new IT systems into DEAR. We asked OCIO officials for documentation of oversight policies and procedures. In response, the OCIO provided a PowerPoint presentation that documented the process flows for when an IT system is added or deleted from the inventory, but did not provide written policies or procedures that are actually in place and being followed. Further, OCIO officials stated that they are generally notified about new systems via email from the bureaus and that they generally review the data for reasonableness. However, we noted that there are no policies or procedures requiring bureaus to report new additions or requiring OCIO to timely review them. This creates the opportunity for a system to be added for which OCIO is unaware, and could lead to incomplete or inaccurate information on the system.

OCIO officials stated that new controls will be incorporated into DEAR that will require the CIO or a designate to authorize all system additions and will automatically notify OCIO when a system has been added to DEAR. These system enhancements should help improve the reliability of data on new systems; however, OCIO will need to document the procedures it will perform once notified of a system addition.

Ensuring All Systems in the Inventory Are Mapped to an Accreditation Boundary

In our report *Annual Evaluation of the Department's Information Security Program* (NSM-EV-MOI-0013-2005), we reported that DOI was in the process of matching IT systems in the certification and accreditation inventory maintained in the Command Center system to the DOI-wide IT systems inventory maintained in DEAR. There was not a one for one matching between these inventories because IT systems separately identified in the DEAR inventory were often combined into a "parent system" for purposes of certification and accreditation. DOI completes accreditation packages for each "parent system."

In early 2006, OCIO merged the inventory of certified and accredited systems into DEAR although the matching had not yet been completed. DEAR identifies those "parent systems" as "accreditation boundaries." *OCIO Directive 2006-09* requires that all IT systems in DEAR be mapped to an associated accreditation boundary within DEAR. At the time of our review, there were 257 systems in DEAR that were not yet mapped. Of the 257 systems not mapped, 104 were from NPS. The enterprise architect at NPS stated that a reconciliation of these systems was ongoing and 70 of these systems had been eliminated or mapped to existing accreditation boundaries as of April 2006, leaving 34 systems still unmapped.

This situation makes it possible for the OCIO to not know whether those remaining systems have undergone the required certification and accreditation process. This condition leaves DOI potentially vulnerable to information security weaknesses. OCIO maintains that progress is being made toward resolving the issue of all systems not designated in DEAR as being certified and accredited. We agree that progress has been made but believe that more diligence is necessary to ensure that all systems in DEAR are mapped to an accreditation boundary as soon as possible.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. Develop and implement policies and procedures that require bureau CIOs to certify the completeness and accuracy of their bureaus' inventory data in DEAR on an annual basis.

2. Mandate consistent DOI-wide procedures for maintaining IT systems inventory or require bureaus CIOs to document their individual procedures for implementing OCIO's general guidelines.

3. Document OCIO procedures for providing oversight to the inventory process.

4. Complete the mapping of all IT systems in DEAR to an accreditation boundary.

Appendix 1

Scope and Methodology

We reviewed the IT systems inventory processes at OCIO and three bureaus to determine whether DOI has an adequate process for inventorying its IT systems by interviewing staff responsible for the oversight and maintenance of IT systems inventories. In addition, we:

- reviewed laws, policies, procedures, and guidance relating to IT systems inventories;
- reviewed current and proposed processes for the maintenance of IT systems inventories and selected security controls; and
- reviewed prior audit and evaluation reports, Government Performance and Results Act goals, and Departmental Performance and Accountability Reports to determine whether they discussed issues relating to IT systems inventories.

We conducted our evaluation from December 2005 through March 2006 and reviewed the IT system inventories as of February 3, 2006. We did not evaluate the actual accuracy or completeness of the IT systems inventory in DEAR. In addition, we did not review the inventory processes for any national security-related systems.

Our evaluation was performed in accordance with the *Quality Standards for Inspections,* dated January 2005, issued by the President's Council on Integrity and Efficiency.

During this evaluation, we conducted onsite work at the following office and bureaus:

Department of the Interior

Office of the Chief Information Officer	Washington D.C.
Bureau of Land Management	Lakewood, CO
National Park Service	Washington D.C.
U.S. Geological Survey	Reston, VA

PRIOR AUDITS AND EVALUATIONS

The Office of Inspector General (OIG) has reported on DOI's IT system inventory processes as part of our annual FISMA reporting. The following report contained specific areas related to our current evaluation:

- ***Annual Evaluation of the Department's Information Security Program,* OIG Report No. NSM-EV-MOI-0013-2005, October 2005.**

  The report stated that DOI did have an IT inventory system in place but still relied on manual efforts to reconcile various systems counts and used a separate inventory for its certified and accredited IT systems. OIG generally agreed with the number of IT systems contained in the inventory. While no IT systems were found missing from the inventory, OIG did not believe that DOI had an efficient inventory process in place. Further, OIG was concerned about the various different inventories used to report IT system counts.

During the past 5 years, the Government Accountability Office (GAO) has not issued any reports specifically related to DOI's IT systems inventories. However, it issued the following report on IT investment management:

- ***Bureau of Land Management: Plan Needed to Sustain Progress in Establishing IT Investment Management Capabilities*, Report No. GAO-03-1025, September 2003.**

  GAO reported that the Bureau of Land Management (BLM) had made progress in establishing its IT investment management capabilities, but still needed to develop and implement a plan to guide its efforts in the IT investment management area. GAO recommended that this plan include specific measurable goals, outcomes, and needed resources, and assign clear responsibility for tasks. Further, the report stated that BLM had not defined policies and procedures for collecting information into the Budget Planning System in order to help it make informed investment management decisions. A key practice cited in the report is the need for establishing policies and procedures for identifying IT projects and systems and collecting, in an inventory, information about the IT projects and systems that is relevant to the investment management process.

Appendix 3

ACRONYMS AND ABBREVIATIONS

BEAR	Bureau Enterprise Architecture Repository
BLM	Bureau of Land Management
C&A	Certified and Accredited
CIO	Chief Information Officer
DEAR	DOI Enterprise Architecture Repository
DOI	Department of the Interior
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IT	Information Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
USGS	U.S. Geological Survey

Report Fraud, Waste, Abuse and Mismanagement

Fraud, waste, and abuse in government concerns everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular area programs and operations. You can report allegations to us in several ways.

By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 5341 MIB
1849 C Street, NW
Washington, D.C. 20240

By Phone:

24-Hour Toll Free	800-424-5081
Washington Metro Area	703-487-5435

By Fax: 703-487-5402

By Internet: www.doioig.gov

Revised 07/06