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

FY 2009 FISMA EVALUATION REPORT

Report No. ISD-EV-MOA-0001-2009

November 16 2009 (Revised)

Table of Contents

Acronyms and Other Reference Terms

ABACIS ..... Advanced Budget/Accounting Control and Information System
AMLIS ..... Abandoned Mine Land Inventory System
AM-LAN ..... Aviation Management Local Area Network
AO……...Authorizing Official
AUP…….Acceptable Use Policy
BIA..... Bureau of Indian Affairs
BLM..... Bureau of Land Management
BOR ..... Bureau of Reclamation
C&A..... Certification and Accreditation
CIGIE ..... Council of the Inspectors General on Integrity and Efficiency
CIO..... Chief Information Officer
CIRC ..... Computer Incident Response Capability
CISO ..... Chief Information Security Officer
CISSP…….....Certified Information Systems Security Professional
COOP ..... Continuity of Operations Plan
CSAM ..... Cyber Security Assessment and Management
CSD..... Cyber Security Division
DAR……..Data at Rest
DEAR..... Departmental Enterprise Architecture Repository
Department..... Department of the Interior
DOI ..... Department of the Interior
EHP……...Earthquake Hazards Program
ESN ..... Enterprise Services Network
EZGSS ..... Eastern Zone General Support System
FAIMS ..... Federal Aid Information Management System
FBMS..... Financial and Business Management System
FDCC ..... Federal Desktop Core Configuration
FIPS ..... Federal Information Processing Standards
FISMA ..... Federal Information Security Management Act
FISSA..... Federal Information System Security Awareness
FFMIA……..Federal Financial Management Improvement Act
FMFIA ..... Federal Managers Financial Integrity Act
FOUO……For Official Use Only
FTP..... File Transfer Protocol
FWS ..... U.S. Fish and Wildlife Service
FY ..... Fiscal Year
GOS ..... Geospatial One Stop
GSN……..Global Seismic Network
GSS ..... General Support System
IATO ..... Interim Authority to Operate
IBiS ..... Integrated Business Solutions
ICR..... Internal Control Review
IG……...Inspector General
ISA ..... Interconnection Security Agreement
ISD ..... Information Security Division
IT..... Information Technology
MMS ..... Minerals Management Service
NBC ..... National Business Center

NBC-EP .....National Business Center Enterprise Portal
NIIMS .....National Irrigation Information Management System
NFR…….Notice of Finding and Recommendation
NPS ..... National Park Service
NIST.....National Institute of Standards and Technology
NMRP .....National Map Reengineering Project
NFPORS ..... National Fire Plan Operations and Reporting System
OAG.....Office Automation Generalized
OAS .....Office Automation Specialized
OCIO..... Office of the Chief Information Officer
OCS……Outer Continental Shelf
OIG ..... Office of Inspector General
OHA..... Office of Hearing and Appeals
OHANet ..... Office of Hearing and Appeals Network
OHTA ..... Office of Historical Trust Accounting
OneGSS ..... National Park Service General Support System
OMB .....Office of Management and Budget
OS .....Office of the Secretary
OSM.....Office of Surface Mining
OST……Office of the Special Trustee
PHB..... DOI IT Security Policy Handbook
PIA ..... Privacy Impact Assessment
PII..... Personally Identifiable Information
POA&M.....Plan of Action and Milestones
RBST .....Role-Based Security Training
RIDB..... Recreation Information Database
RMSS.....Reclamation Mission Support System
ROB ..... Rules of Behavior
ROS.....Recreation One Stop
SLA…….Service Level Agreement
SOL……...Office of the Solicitor
SP ..... Special Publication
SSP..... System Security Plan
STIG.....System Technical Implementation Guide
ST&E ..... System Testing and Evaluation
US-CERT.....U.S. Computer Emergency Readiness Team
USGS ..... United States Geological Survey
WCVF..... Weakness Completion Verification Form

Results in Brief

The Department of the Interior (DOI) does not fully comply with the Federal Information Security Management Act (FISMA) again this year. The decentralized organizational structure, fragmented governance processes related to the Information Technology (IT) program, lack of oversight, bureau resistance to Departmental guidance, and use of substantially under-qualified personnel to perform significant information security duties exasperates the challenges in securing the Department's information and information systems. Personnel responsible for management of the IT Programs are not accountable for results, and existing investments are not leveraged to their full potential. These serious flaws significantly negate the benefit of the $182 million spent on IT security in fiscal year (FY) 2009 and the efforts of the 677 employees and contractors fully devoted to information security across the Department.

Delegation of authority regarding IT security leads to a decentralized organizational structure within the Department. In contrast to requirements in the Clinger-Cohen Act and FISMA, Secretarial Order 3244, *Standardization of Information Technology Functions and Establishment of Funding Authorities*, created an individual Chief Information Officer (CIO) for each organization within the Department with 5,000 or more employees. Secretarial Order 3244 states all bureau and office CIO organizations are fully responsible for technology management, security management, information management, telecommunications management, inventory and asset management, strategic planning, project management, and IT career/skills management. We found bureau and office CIOs had little or no control over these functions, personnel performing these functions, or budgets funding these functions within their organizations. We also found these functions further delegated within individual bureaus and offices to regional, district, or program managers. Delegating authority from the Department CIO has resulted in multiple layers of bureaucracy that impede achievement of results and drive up costs. We continue to recommend the revocation of Secretarial Order 3244 and recommend the authority for managing IT security be realigned solely under the Department CIO.

We noted bureau and office resistance was a major hurdle to achieving results. In August 2006, the Department CIO directed all bureaus and offices to transition to the Department's remote access system by January 31, 2007. As of June 2009, BLM, BOR, NBC, NPS, and USGS still maintained separate systems. In-fact, BLM continues to expand its remote access system.

The governance framework within the Department is inefficient, wasteful, and lacks accountability. The Information Technology Management Council (ITMC) is the current governing body for IT within DOI and is comprised of the bureau and office CIOs. These CIOs report to individual bureau and office directors. We found ITMC generally responsible for making decisions that impact information security Department-wide. Implementation of ITMC decisions is sporadic and often incomplete. Delegating governing authority to ITMC is inconsistent with law and federal policy and has led to waste and a decrease in accountability. The lack of adequate governance constitutes a weakness in the Department's overall information systems security program, which is a significant deficiency under FISMA. We recommend overhaul of the governance processes related to IT and IT security, and while DOI has researched and

discussed new IT governance frameworks throughout 2009, no changes from recommendations offered in previous years have been applied.

In addition, oversight in the Department is materially absent despite technology that enables it. We found examples of weaknesses in the Department's information security program abundant and obvious. Many of the weaknesses we identified went unrecognized by the Department itself. Investments, such as the Cyber Security Assessment and Management (CSAM) tool and the Departmental Enterprise Architecture Repository (DEAR), provide information to Department personnel charged with oversight. We found, however, that quality and accuracy of the data provided to them went unverified. Unverified status updates in CSAM led to inadequate resolution of previously documented weaknesses, and failure to review data in DEAR left obvious weaknesses in system certification and accreditation (C&A) unrecognized. Quality review and verification activities have not occurred and thus we found Departmental oversight of its information security program ineffective.

We also noted bureau and office resistance was a major hurdle to achieving results. For example, we observed a project meeting related to the Enterprise Active Directory Operational Standardization Project in which bureau representatives stated they would not share their information with the Department. Furthermore, in August 2006, the Department CIO directed all bureaus and offices to transition to the Department's remote access system by January 31, 2007. As of June 2009, the Bureau of Land Management (BLM), Bureau of Reclamation (BOR), National Business Center (NBC), National Park Service (NPS), and United States Geological Survey (USGS) still maintained separate systems, and BLM continued to expand its system. We found the Department had spent approximately $900,000 on the Internet Security Systems (ISS) vulnerability scanning system through April 2009, but only four bureaus and offices; BOR, Office of Hearing and Appeals (OHA), Office of Surface Mining (OSM), and Office of the Solicitor (SOL); were using the system to conduct vulnerability scanning of information systems under their control. The Bureau of Indian Affairs (BIA), BLM, U.S. Fish and Wildlife Service (FWS), NBC, NPS, Office of Historical Trust Accounting (OHTA), and USGS procured and implemented their own separate solutions. Managing individual solutions results in inconsistent implementations. During the FY 2009 financial statement audits, NFR USGS-2009-007 was issued when multiple systems were identified as not having the latest software security patch installed and the software had been mis-configured.

In our FY 2008 FISMA report, we stated, "The Department has seemingly delegated performance of significant information security duties to personnel who are likely ill-prepared to perform the task." In FY 2009, we again found many personnel reported as performing significant information security responsibilities who held positions with job titles not synonymous with information security. For example, the Department reported a GS-15 "Pipeline Coordinator Officer," a GS-14 "Supervisory Land Law Examiner," a GS-5 "Administrative Clerk," three GS-7 "Budget Technicians," a GS-7 "Purchasing Agent," a GS-9 and a GS-13 "Contract Specialist," and a GS-7 "Personnel Specialist" were all 100 percent devoted to performing significant information security duties.

FISMA requires that personnel with significant responsibilities for information security receive role-based security training (RBST). During FY 2009, we determined 3,531 employees and contractors across the Department required RBST training. Our evaluation found 89 percent of their RBST self-certified training was completed. We found the Department did not verify that any of the RBST self-certified training was relevant or actually completed. In our verification activities, we found the Minerals Management Service (MMS), NBC, Office of the Secretary (OS), and SOL could not provide any evidence supporting that the RBST self-certified training had actually been completed. In our review of artifacts provided by other bureaus and offices, we found only 13.5 percent of the self certifications were actually relevant and complete. We determined routine operational activities were being reported as training. For example, the BOR CIO was given credit for training because he received routine briefings related to security goals and objectives. We further found coursework on developing performance standards, hostile work environments, and use of the Department's travel reservation system counted as information security training.

Lack of funding, however, is not the most critical problem. In 2006, the Office of Management and Budget (OMB) directed federal agencies to encrypt data on mobile computers/devices under certain circumstances. In December 2008, the Department purchased thousands of licenses for software in support of this requirement, but the software was never implemented. Based on our estimate, the Department is losing more than $57,000 per month in value due to deprecation of the software licenses.

The annual audit of DOI financial systems includes an assessment of the Federal Information System Controls Audit Manual (FISCAM) internal controls and internal vulnerability assessments of the financial systems. The majority of the Notice of Findings and Recommendations (NFR) from that audit are associated with information technology control weaknesses. Moreover, vulnerability scanning of those systems identified 36 vulnerabilities that were categorized as high and 52 as medium. Those vulnerabilities present risks to DOI financial systems and data integrity.

Our assessment of a subset of DOI systems identified that the greatest concentrations of weaknesses were in system inventory and contingency plan testing. Figure 1 presents a comparison of FY 2007, FY 2008, and FY 2009 levels of compliance across key FISMA areas. We noted improvements, but not yet full compliance; for annual self- assessments, certification and accreditation (C&A), privacy impact assessments and configuration management. We identified ongoing deficiencies in system inventory, system impact levels, contingency plan testing, Plan of Actions and Milestones (POA&M), incident response and training and awareness. We determined that bureaus and offices continue to have implementation inconsistencies across all key FISMA areas.

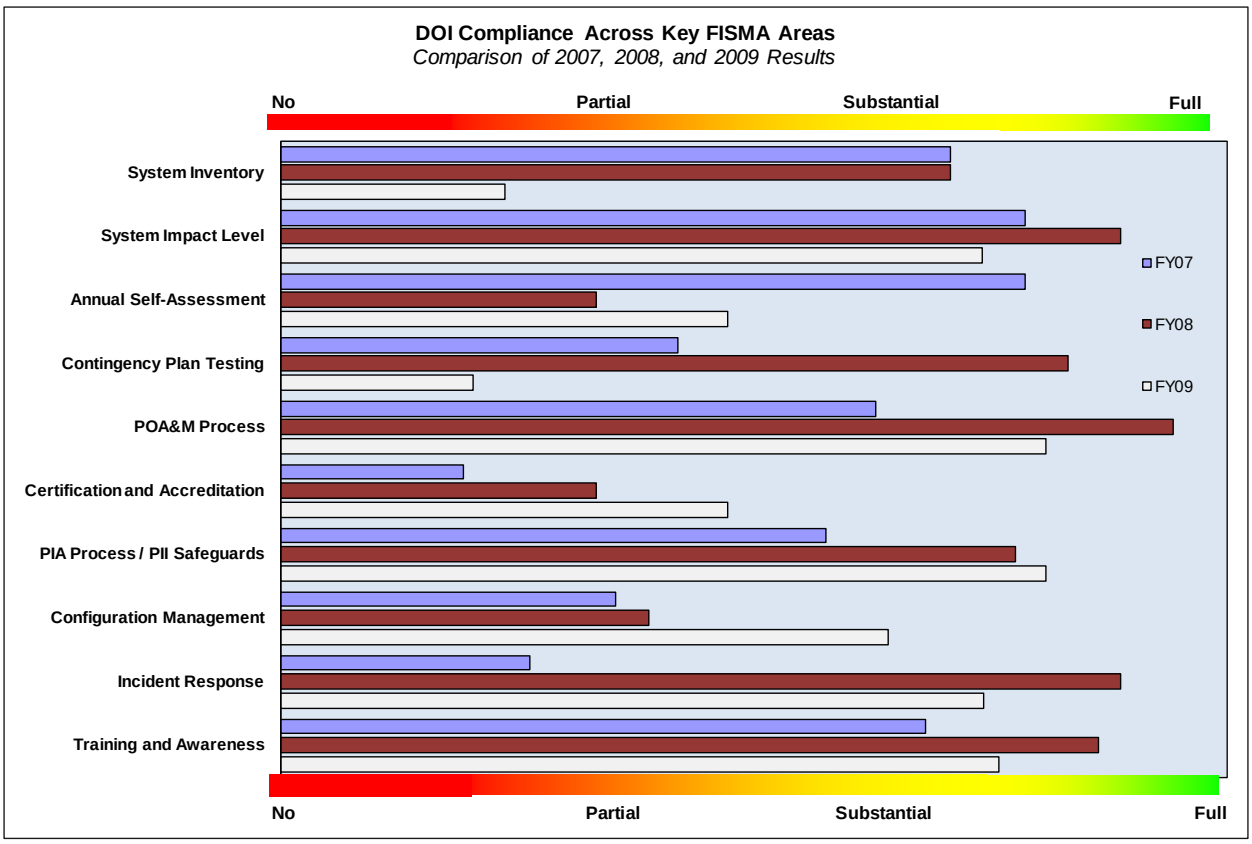

Figure 1: Comparative Results of Reviews

Of the 14 systems in the FISMA subset; ten had inconsistencies in the system inventory identified in DEAR and the system security plans. Twelve contingency plans were either not tested or the tests were not completed in accordance with Departmental policy. The C&A process showed some improvement, however implementation inconsistencies persist and oversight at the Departmental level has failed to identify and insure corrective actions.

We include many recommendations from previous reports to address the deficiencies identified throughout this report. Until the Department establishes a sound governance structure for its IT program, creates an atmosphere of accountability, and performs adequate oversight, it is unlikely information security will improve.

Introduction

The DOI is a decentralized, cabinet-level agency of the federal government. It manages about one-fifth of the land area of the United States and all of the nation's Outer Continental Shelf (OCS). DOI is the nation's principal conservation agency dedicated to protecting America's treasures for future generations by providing access to our nation's natural and cultural heritage. DOI honors all trust responsibilities to American Indians, Alaska Natives, and our responsibilities to island communities. The Department's mission includes: conducting scientific research, providing wise stewardship of energy and mineral resources, fostering sound use of land and water resources, serving as the largest supplier and manager of water in 17 western states, conserving and protecting fish and wildlife, and offering recreation opportunities. Eight bureaus and each of the Departmental offices carry out the Department's missions.

In August 2002, the Secretary of the Interior issued a memorandum, *Information Technology Resources Management,* establishing the ITMC, which is the governing body for information technology within DOI. In addition, in November 2002, the Secretary signed order number 3244. Secretarial Order 3244 established an individual CIO for each organization within the Department with 5,000 or more employees. The bureau and office CIOs established by the order report to bureau directors and deputy directors. Bureau and office CIOs, as well as the Department CIO, form the ITMC.

In FY 2009, the Department reported 223 information systems[1] in their IT system inventory, including major applications and General Support Systems (GSS). The information systems support various DOI program and mission areas, such as National Critical Infrastructure, Indian Trust Management, Financial Management, Law Enforcement, Facilities and Maintenance, and customer oriented business operations. The Department CIO was not the accrediting official for most of the information systems in the Department's inventory.

In FY 2009, the Department had an overall budget of $17.1 billion and reported 67,000[2] employees. DOI's total IT Investment Portfolio for FY 2009 was $965 million[3] (or roughly 5.6 percent of DOI's overall budget). Based on FY 2009 DOI Exhibit 53, $182 million (or 18 percent of the IT Investment Portfolio) was budgeted to IT Security. Only a fraction of this budget was under the purview of the Department CIO. During FY 2009, the Department reported 3,531 employees and contractors across the Department performed significant responsibilities for information security. Only a fraction of these personnel were under the purview of the Department CIO. Compared to FY 2008, the Department reported 88 additional personnel fully devoted to performing significant information security duties, for a net increase of 14.9 percent.

[1] The 223 systems includes accredited systems, as well as systems with identifiers such as "unmatched", "pending", "blank", and "unknown" that had associated systems or components.
[2] http://www.doi.gov/budget/2010/10Hilites/overview.pdf
[3] FY 2009 DOI Exhibit 53

Background

Congress enacted Title III of the E-Government Act of 2002, commonly referred to as FISMA, in response to concerns about the security of federal information and information systems. FISMA's primary intent was to facilitate progress in correcting agency information security deficiencies and improve the oversight of federal information security programs. Section 3545(a) of the Act requires the Office of Inspector General (OIG) to perform an annual evaluation of the Department's information security program and practices.

FISMA requires the Secretary of Commerce to prescribe standards and guidelines pertaining to federal information systems and make those standards compulsory and binding. The National Institute of Standards and Technology (NIST) is required to develop Federal Information Processing Standards (FIPS). FIPS are mandatory and define the minimum requirements for information security and system security categorizations. OMB must report annually to Congress on agency compliance with FISMA's requirements. This narrative report summarizes the results of our FY 2009 Evaluation of DOI's IT Security Program, as well as our recommendations to assist them in enhancing their information security program and efficiently achieving full compliance with FISMA. We based our results and recommendations on the review of 18 agency systems and evaluations conducted at 11 of the Department's bureaus and offices throughout FY 2009.

FISMA Evaluation Results

We selected an initial subset of 18 DOI IT systems for review. We performed a cursory review of the C&A packages for those systems to ensure they satisfied the minimum criteria to justify a detailed assessment. Based on our cursory review, we excluded four systems from the original sample because they contained fundamental flaws. One system of the four systems we excluded belonged to U.S. Fish and Wildlife Service (FWS) and three belonged to United States Geological Survey (USGS). As a result, we were unable to review any systems from FWS or USGS.

Foundational C&A Weaknesses

We excluded four IT systems, Federal Aid Information Management System (FAIMS), Office Automation Generalized (OAG), Office Automation Specialized (OAS), and National Map Reengineering Process (NMRP) from our initial subset of systems for the following reasons:

1. FAIMS is a highly integrated national automated system for federal assistance grant program administration at FWS. We found FAIMS had the wrong security categorization. The documentation provided by FWS indicated the system was categorized as low impact. Based on the detailed description included in the documentation provided by FWS, we determined that the system should have been categorized as a moderate impact system. The error in establishing the FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, security categorization impacts most of the other C&A documents and further review was not warranted.

2. OAG is a collection of many systems at USGS. We selected the Integrated Business Solutions (IBiS) system for review. IBiS supports the Science Information and Education Office in distribution of all USGS published materials such as maps, books, and scientific reports. This web-accessible service serves internal and external customers around the world, including a network of more than 1800 business partners who resell USGS products. We found IBiS is not properly accredited to operate. Our review found that the accrediting official of record departed from USGS more than two years earlier and subsequent accrediting officials had not accepted the risks associated with continuing operation of the system. Moreover, we found the security categorization of OAG as a whole is defined as moderate impact, while individual subsystems are defined as high impact. FIPS 199[4] requires a system categorization based on the highest value of any included subsystem.

[4] FIPS 199, Paragraph 3, states "For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system."

3. OAS is a collection of systems that provide support for science mission computing activities of distributed projects and applications at USGS. OAS contains 107 systems. We found OAS is not properly accredited to operate. Our review found that the accrediting official of record departed from USGS more than two years earlier and subsequent accrediting officials had not accepted the risks associated with continuing operation of the system. Moreover, we determined that the C&A package is so complex and cumbersome that it is unmanageable. The package as a whole incorporates more than 100 subsystems supporting such critical scientific programs as biology, earth science, water research and monitoring, earthquake monitoring and research, and volcano science distributed across the nation. Subsequent to our initial review of OAS, USGS retired this system, and we later found USGS reassigned the more than 100 systems to a new accreditation boundary.

4. NMRP C&A documentation states that NMRP at USGS "is the complex set of computer systems and telecommunications resources required to acquire, manage, archive and deliver *The National Map* Reengineering Project data." NMRP is a major OMB e-Government initiative and DOI is the managing partner. In our review of the C&A package, we were unable to determine the system's accreditation boundary. The C&A package contained numerous errors and conflicting statements. Therefore, we were unable to determine the purpose of the system with enough understanding to determine if it was properly categorized in accordance with FIPS 199. For example, the NMRP C&A package stated, "These component systems are general support systems and major applications that run on these general support systems." The system must be either a GSS or a major application, not both.[5] Since we could not evaluate the accuracy of NMRP's system categorization, further review was not possible.

During our selection of a subset of systems, we determined USGS did not have any IT systems identified as high impact systems. FIPS 199 defines a high impact system as, "a severe or catastrophic adverse effect, [such as] the loss of confidentiality, integrity, or availability [that] might: ... (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries."

We reviewed public USGS websites and identified multiple programs of critical importance that are supported by IT systems with a consistent level of criticality. For example, USGS programs include:

- Global Seismic Networks (GSN) - Contains 128 seismographic stations in more than 80 countries on all continents; provides coverage for earthquake monitoring, worldwide reporting and research; monitors nuclear explosions worldwide;

[5] NIST 800-18 Revision 1 *Guide for Developing Security Plans for Information Technology System*, section 1.5, states all systems must be "labeled as a major application or general support system."

- Toxic Substances Hydrology Program - Provides objective scientific information on environmental contamination to improve characterization and management of contaminated sites, **to protect human and environmental health,** and to reduce potential future contamination problems;

- Earthquake Hazards Program (EHP) - Provides and applies relevant earthquake science information and knowledge **for reducing deaths, injuries, and property damage from earthquakes** through understanding of their characteristics and effects and by **providing the information and knowledge needed to mitigate these losses.**

On April 3, 2009, we issued a memorandum, *Systems not Prepared to Protect Public Safety*, to USGS stating our concern and questioning why USGS did not have any systems with a high security categorization. Having a moderate rather than a high system categorization artificially lowers the reported risk. By categorizing a system as moderate impact rather than high impact, federal guidance allowed USGS to implement 67 fewer IT security controls. Documentation for the OAS system justified lowering the categorization from high to moderate by stating, "Furthermore, no written formal agreements have been established with external organizations where USGS information is legally required to protect human lives or directly provide for national security."

System Inventory

DOI's system inventory is inaccurate. The inventory is not being timely certified by the bureau CIOs as required by Departmental guidance. We determined system inventory disparities existed between DEAR and the actual system C&A documentation. Half of the components in our sample that are associated with an accreditation boundary have not been documented in the corresponding System Security Plans (SSP). We communicated these inconsistencies to the Department CIO in the April 27, 2009 memorandum, *Management Advisory-Deficiencies in System Inventory Management*. The CIO subsequently advised bureaus to take corrective action by August 21, 2009.

Bureau and office CIOs are not certifying their inventory as required by Departmental guidance. The Department failed to take any action to improve accountability as a result of the failure to timely certify. Office of the Chief Information Officer (OCIO) Directive 2009-002, *Population and Maintenance of the DEAR*, February 6, 2009, required the maintenance of system inventory information and stated bureau CIOs were responsible for ensuring and certifying annually by March 31, 2009, in writing, that the data in DEAR is accurate and complete. We requested copies of the CIO certifications. As of June 15, we received six certifications and did not receive CIO certifications from BIA, NBC, OHA, FWS, OHTA, Office of the Special Trustee (OST), OS, and SOL. The late and missing CIO certifications are indicative of the weak governance and oversight processes in place at the Department.

FISMA section 3544(a)(1)(A)(ii) requires agencies to develop and maintain an inventory of major information systems operated by or under the control of such agency, as well as to identify systems used or operated by contractors and other organizations on behalf of the agency. OCIO Directive 2009-002 requires that inventories include identification of the interfaces between each system and all other systems or networks.

OCIO Directive 2009-002 also states, "The CIOs are also responsible for ensuring that accreditation boundaries include either one General Support System or one Major Application, include all associated minor applications and record security categorizations consistent with the corresponding system security plan." We determined not all minor applications are consistently included in DEAR and in the security documentation. Failing to identify all minor applications makes the accreditation boundaries inaccurate.

Departmental processes for managing inventory and related C&A documentation is complex and duplicative. Both CSAM and DEAR contain system inventory information and supporting C&A data. We found data between DEAR and CSAM were inconsistent.

The *DOI IT Security Policy Handbook* requires bureaus and offices to track all IT system components and security status' by maintaining a comprehensive inventory in DEAR. OCIO Directive 2009-002 establishes "DEAR as the official data source for the entire Department of the Interior (DOI) enterprise architecture artifacts, all DOI information systems and associated attributes related to privacy and Individual Indian Trust Data, and all associations between information systems and accreditation boundaries." The Directive also states that CIOs are responsible for annually ensuring in writing that data in DEAR is accurate and complete.

Furthermore, the September 23, 2008 Departmental memorandum, *Mandatory Use of the Cyber Security Assessment Management (CSAM) Solution*, signed by the Acting Department CIO, specifies the mandatory usage and full implementation of the CSAM solution. CSAM is the official repository for preserving C&A Package documentation, POA&M, and Internal Control Reviews (ICR) for each system in inventory. General system inventory information is also included in CSAM as it correlates to the security documentation.

System Impact Level

In addition to FIPS 199, and in compliance with FISMA, NIST further provided procedures for determining the security categorization of a system in Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. SP 800-60 provides guidance to assist federal agencies in categorizing information and information systems into high impact, moderate impact, or low impact systems, and the category rating determines the required security controls.

Of the 14 systems evaluated, we found 11 systems categorized as moderate impact and three categorized as low impact. We determined that documentation supported 11 of the 14 (79 percent) security categorizations. We found documentation for two systems did not provide evidence that all relevant data types were considered in determining the FIPS 199 categorization. Moreover, one GSS did not document the process used to ensure all information types at each component location had been considered in making the determination. Quality assurance review of the C&A documentation at the Department level could have detected these errors.

Annual Self-Assessment

FISMA section 3544(b)(5), requires annual assessments of the effectiveness of information security policies, procedures, practices, and security controls for all systems. OCIO Directive 2009-004, *Internal Control Review* (ICR), February 5, 2009, provides Departmental guidance for completing annual self-assessments for systems. Mandatory use of CSAM was required beginning second quarter FY 2009 for all ICRs. Thus, the ICRs we reviewed were completed using the templates used prior to the CSAM application.

We determined that 13 of 14 systems reviewed had undergone an annual self-assessment within 12 months of their FY 2008 annual self-assessment. The quality of these reviews varied widely. In many instances, assessment procedures were not documented and descriptions of implementation plans were not provided for the assessed controls. In addition, we noted many cases where weaknesses in security controls were identified, but the weakness was not captured as either a program or system-level POA&M as required by DOI policy.

We found that NBC thoroughly documented the assessment results, clearly identified common controls, and cross referenced identified weaknesses to POA&M items.

The NPS' OneGSS did not adequately assess security controls for each component. Thus, the rollup for the system did not accurately reflect the effectiveness of the policies, procedures, and controls for the entire accreditation boundary.

NIST 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems,* states, "It is not feasible or cost-effective to monitor *all* of the security controls in an information system on a continuous basis; the information system owner should select an appropriate subset of those controls for periodic assessment." OMB elaborates in M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, stating agencies "should develop an enterprise-wide strategy for selecting a subset of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three year accreditation cycle." The Department does not have an enterprise-wide strategy for selecting a subset of controls to be assessed each year.

Contingency Plan Testing

FISMA requires IT security programs to have plans and procedures that ensure continuity of operations of information systems. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, provides guidance for establishing, maintaining, and testing contingency plans. Continuity of operations planning ensures that agencies will have the ability to perform essential functions during situations that disrupt normal operations. Departmental policy requires bureaus to conduct tests and/or exercises at least annually to assess the effectiveness of the Continuity of Operations Plan (COOP).

We found four plans were not tested within the past year, two of which are contractor systems. Of the 10 plans that were tested, we determined only 3 were in full compliance with NIST standards and DOI policy. The remaining seven plans failed to adequately document the contingency plan process and test results. We found bureau COOP testing had the following types of issues: scope was limited, objectives of the test were not established, COOP had outdated contact information, lessons learned and results were not documented, and COOP was not consistently updated based on test results.

Plan of Action and Milestones

FISMA requires federal agencies' information security programs to include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices. OMB prescribed the POA&M as a tool for detailing identified weaknesses and planned corrective actions for each federal information system or security program. System-level POA&Ms are documented as part of the C&A process and is a required document in the C&A package.

As of the fourth quarter FY 2008, bureaus and offices used the CSAM system, a web-based application for tracking and reporting system and program-level POA&Ms for all 14 systems we reviewed. Since 2004[6], OMB specifically requires agencies to share POA&Ms with agency Inspectors General (IG) to ensure independent verification and validation of identified weaknesses and completed corrective action. We accessed the CSAM application and supporting processes during our *Verification of Previous OIG Recommendation Evaluation*, report number ISD-EV-MOA-0002-2009. We found documents and supporting artifacts, such as screenshots, uploaded to CSAM did not always support the closure of POA&Ms. The artifacts did not always provide substantive evidence that corrective action was complete. We concluded the Department was not leveraging available information or adequately performing oversight of the POA&M process.

Plan of Action and Milestones Process Standard V1.5, January 28, 2008, provides Departmental guidance for implementing the POA&M process. We further found that each bureau was maintaining individual program-level POA&Ms. FISMA section 3544(a)(3)(B) requires a senior

[6] M-04-25, *FY 2004 Reporting Instructions for the Federal Information Security Management Act*

agency information security officer who develops and maintains an agency wide information security program. Multiple bureaus and offices having their own program-level POA&Ms is indicative of the Department attempting to coordinate multiple programs rather than establishing a single, agency-wide program as required by FISMA.

We identified inconsistencies in implementation of the Department's POA&M guidance. For example, NPS' OneGSS has many weaknesses identified at the component (subsystem) level. Most of the identified weaknesses, however, were never included in the OneGSS POA&M or any other formal tracking system. Without tracking these items, there is little or no assurance that the security weaknesses are receiving the necessary resources or are timely mitigated.

Certification and Accreditation

OMB tasks the OIG to complete a qualitative assessment of the C&A process. NIST provides guidance that establishes a common security authorization process for federal information systems. Our review of the C&A process and related documentation identified key areas that resulted in DOI's noncompliance with FISMA.

After evaluating the C&A process and documentation for the 14 systems, we determined the Department did not use readily available information in order to oversee the C&A process. For example, expired accreditations were allowed to persist, authorizing officials left the agency and new authorization letters were not obtained, and unmanageable accreditation boundaries went unchecked. We identified the following process and documentation weaknesses.

DOI Systems in Inventory without Valid Accreditation

OMB memorandum M-09-29 specifically states that OMB does not recognize interim authority to operate (IATO) for IT systems; either a system is accredited and has authority to operate, or it is not. We reviewed the accreditation status of all systems in DOI's inventory and identified many classifications other than accredited such as: IATO, unmatched, no authority to operate, unknown, not started, in progress, or not applicable. We determined that eight systems have been in one of these unaccredited categories since at least March 14, 2008.

Three systems from the original subset of 18 systems had an accreditation expiring during FY 2009:

- OSM: Abandoned Mine Land Inventory System (AMLIS) expired July 21, 2006, and was not reaccredited until August 3, 2009;

- USGS: Accreditations for OAS and OAG expired July 13, 2009. We later determined USGS retired both systems and transferred their assets to new accreditation boundaries.

One of those systems was "Science and Support System-Moderate" (SSS-M). SSS-M was accredited on July 8, 2009. We traced the transfer of OAG and OAS assets to SSS-M using information available in CSAM. With the transfer of assets, SSS-M became the C&A of record for more than 120 information assets. The new SSS-M C&A documentation in CSAM appears to contain many of the same errors we identified for OAS and OAG. According to the SSS-M C&A package, the newly accredited USGS system requires $26.7 million to mitigate all known weaknesses.

System Authorizing Official Departed

The Authorizing Official (AO) signs the accreditation memo and authorizes the operation of information systems. NIST SP 800-37 states, "By accrediting an information system, an agency official accepts responsibility for the security of the system and is fully *accountable* for any adverse impacts to the agency if a breach of security occurs." In the event the AO departs DOI, no one remains to assume responsibility for the system or to be held accountable for adverse impacts. In one case, we found that the name of the AO for a system managed by NBC was updated in the C&A package, but when we contacted them, they stated they never heard of the system. Updating the C&A documentation with a new name is misleading and does not satisfy the intent of FISMA. We determined that the original AO for five of the 18 systems in our original sample had left DOI years earlier. Subsequent to our identification of this issue, the Department updated guidance to address similar situations.

Unmanageable Accreditation Boundaries

We determined that C&A packages for some very large and complex GSS, including NPS' OneGSS, did not provide enough detail or include all components necessary for a complete C&A package. The GSS documentation covered a large, diverse universe of equipment, locations, and organizational groups. In order to cover all this material in a single package, system descriptions and control statements were vague. The lack of detail and specificity undermined the intent of having a C&A package. We concluded the sheer volume and complexity of the packages alone, if they were done in sufficient detail, would make them unmanageable. Even if done in sufficient detail, however, a single package still may not meet all NIST requirements. For example, many of the individual subsystems were managed by different groups and under various funding authorities. DEAR lists 150 subsystems for OneGSS. We sampled 10 of those subsystems and found six were not identified as minor applications in the OneGSS C&A documentation.

Certification and Accreditation Documentation

FISMA requires agencies to complete C&A documentation for each accredited system. NIST SP 800-37 and NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, provide guidance on quality and content of that documentation.

The AO's authorization means the "official assumes responsibility and is accountable for the risks associated with operating an information system." DOI Secretarial Order 3244 delegated authority for "system accreditation and certification" to individual bureau and office CIOs. The Department CIO was not the accrediting official for most of the information systems in the Department's inventory.

C&A packages throughout DOI are inconsistent; they are completed using a variety of formats. The SSP consolidates data on the IT security controls. Some of the SSPs categorize the controls by class including: management, operational, or technical controls. Other SSPs categorize the controls by control families as found in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. Multiple formats create challenges for monitoring and oversight.

We identified inconsistencies in the determination of the security categorization of the systems in our sample. The process to determine the security categorization is based on the types of information that is stored and processed by the system. Some bureaus and offices consider all information types as specified in NIST SP 800-60. Others document their consideration of only a subset of information types. When consideration of all information types is not documented, it is not possible for an independent reviewer to assure all information types were considered in establishing the security categorization. This variation in format and content impairs the Department's ability to perform adequate oversight.

We found C&A documentation throughout the department with a variety of security classification markings. Some documents are labeled For Official Use Only and others are labeled Sensitive. The inconsistency creates confusion for records management and securing the documents. Furthermore, we observed many signatures on key security documents that we could not identify.

Departmental memorandum, *Mandatory Use of the Cyber Security Assessment Management (CSAM) Solution*, September 23, 2008, designated the CSAM application as the official repository for C&A documentation. We determined CSAM was consistently used for maintaining C&A documentation for our sample of systems. Departmental guidance, *Certification and Accreditation Guide using CSAM V2* was released on June 2, 2009. The templates and checklists available within CSAM provide a structured framework.

System Security Plans

According to NIST SP 800-18, Revision 1, the purpose of an SSP is to consider the general operating environment of the system, provide an overview of the security requirements applicable to the system, and describe the controls in place or planned for meeting those requirements. The SSP is considered the foundational document of the full C&A process and

forms the basis of system authorization. The SSP should be updated at least annually or following any major system and/or organizational change.

We noted a wide variance in the quality of SSPs across our subset of 14 systems. While several SSPs appeared to be comprehensive with up-to-date documents, we identified inaccuracies, inconsistencies, or omissions of information in 13 SSPs. We found instances where the system descriptions were incomplete and did not accurately identify all subsystems or minor applications within the system's accreditation boundary. In nine SSPs, there was either no reference to the security technical implementation guides for the infrastructure supporting the system, or the reference was vague. Moreover, some SSPs did not identify or thoroughly address bureau or office-level common security controls having direct impact on the system's security posture.

Three of the 14 systems we reviewed in detail were identified in DEAR as being operated by contractors: Recreation Information Database, National Fire Plan Operations and Reporting System, and National Irrigation Information Management System (NIIMS). Our assessment of those systems noted the C&A documentation did not clearly identify the systems as being operated by a contractor. For those systems, there was insufficient detail within the C&A package to assess bureau oversight of the contractor. For example, the annual security self-assessments for these systems did not identify or include assessment of the controls at the contractor facility. The respective SSPs did not clearly distinguish controls implemented by the bureau from those implemented by the contractor. Only one of the SSPs actually identified the contractor.

IT security controls are associated to an accredited system based on the FIPS 199 security categorization of the system. We assessed 14 SSPs to determine if the appropriate security controls were identified and if the description of the control implementation, as well as the roles and responsibilities, were adequate. We concluded 89 percent of the required IT security controls were actually included in the SSPs. We further concluded 72 percent of the controls were adequately described in the SSPs. Appendix 3 provides additional details of our assessment of security controls by individual systems.

Risk Assessments

Under FISMA, agencies are responsible for (a) providing security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems; and (b) establishing policies and procedures that ensure information security is addressed throughout the life cycle of each agency information system. NIST SP 800-30, *Risk Management Guide for Information Technology Systems,* sets forth a nine-step risk assessment methodology, and the *DOI IT Security Policy Handbook* directs bureaus and offices to comply with this methodology.

We found all 14 systems we reviewed had completed the initial risk assessment in accordance with NIST 800-30. We determined, however, that risk assessments for half of the systems did not document the continuous monitoring efforts, the results and security impact of those efforts, or the process to mitigate risks. Six of the 14 systems we reviewed did not adequately document how the controls were assessed and how the risks were managed. For example:

- BIA identified "*Unauthorized access to NIIMS"* as the only threat to NIIMS in the system Risk Assessment Matrix. The recommended control was "examine NIIMS's in-place service level agreement (SLA). Ensure that it addresses BIA procedural requirements for maintaining accountability of granting, reviewing, and terminating NIIMS system access, as well as address any BIA reporting requirements regarding NIIMS system operation and administration by NBC." The recommended control does not address the identified risk. Furthermore, the description does not identify how the controls were monitored or the results and corrective actions to mitigate the risk.

- Office of Hearing and Appeals Network (OHANet) risk assessment included the results from Technical Vulnerability Assessment and other reviews of the security controls; yet, the risk assessment did not document the status of corrective action. One section of the risk assessment identified 11 vulnerabilities classified as high risk, implementation (yes or no) was blank, and the action responsibility was not assigned.

Quality Assurance Reviews

The Department's compliance reviews and the OIG systems assessments routinely result in conflicting conclusions. DOI's Cyber Security Division (CSD) conducts annual reviews as part of the Department's FISMA oversight and compliance efforts. CSD reviews system C&A packages, as well as components of the IT security program. CSD's quality assurance reviews do not reliably detect systemic weaknesses in the bureaus' security documentation. While our reviews noted numerous errors and inconsistencies in the bureaus' C&A packages and supporting security documentation, CSD compliance reviews resulted in perfect, or near perfect, scores. The breadth and depth of Departmental oversight and compliance reviews are lacking.

Continuous Monitoring

NIST SP 800-37 defines the continuous monitoring phase of the C&A process and states, "Monitoring the risk assessments, system security plans, and security assessments play an important role in security accreditation. It is essential that agency officials have the most complete, accurate, and trustworthy information possible on the security status of their information systems in order to make timely, credible, risk-based decisions on whether to authorize operation of those systems." Continuous monitoring should occur throughout the system life cycle. An effective continuous monitoring program includes:

- configuration management and control processes for information systems;

- security impact analyses on actual or proposed changes to information systems and environments of operation;

- assessment of selected security controls based on continuous monitoring strategy;

- security status reporting to appropriate organizational officials; and

- active involvement by authorizing officials in the ongoing management of information system-related security risks.

We concluded that the Department has not achieved a comprehensive, integrated continuous monitoring capability. Furthermore, we concluded that DOI has not yet developed and acted on a strategy for implementing a comprehensive, integrated continuous monitoring capability. We found that various bureaus and offices, and regions and districts within individual bureaus and offices, had implemented various technical capabilities in a variety of formats using different products, but this fragmented approach often results in systems that do not communicate with each other and frequently requires manual intervention to analyze data and generate reports. For example, we found that the Department had spent approximately $900,000 on the Internet Security Systems (ISS) vulnerability scanning system through April 2009. Only four bureaus and offices; BOR, OHA, OSM, and SOL; were using the system to conduct vulnerability scanning of information systems under their control. BIA, BLM, FWS, NBC, NPS, OHTA, and USGS procured and implemented their own separate solutions.

We noted that bureau and office resistance was a major hurdle in achieving results. For example, we attended a project meeting related to the Enterprise Active Directory Operational Standardization Project, which was voted on and approved by the ITMC in 2008. During the meeting, Departmental staff asked the MMS representative why MMS was not yet connected to the Department's central servers. The MMS representative responded, "We don't want you to have that information." In August 2006, the Department CIO directed all bureaus and offices to transition to the Department's remote access system by January 31, 2007. As of June 2009, BLM, BOR, NBC, NPS, and USGS still maintained separate systems.

The Department initiated an effort to establish a Security Operations Center within OCIO to organize and consolidate technical monitoring and incident response. As we concluded in previous years, until the Department consolidates the many systems, better organizes human resources, and aligns management authority to streamline decision-making, it is unlikely they will achieve and sustain material improvement.

Interconnection Security Agreements

An Interconnection Security Agreement (ISA) defines the responsibilities and technical security requirements of interconnecting DOI IT systems to nonagency systems. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, provides a management approach for interconnecting IT systems with an emphasis on security. The *DOI IT Security Policy Handbook* states interconnections must be documented in the SSP. DOI does not provide specific guidance regarding the need for an ISA between the bureaus and offices and Enterprise Services Network (ESN), or the need for DOI as the managing partner on e-government initiatives to manage ISAs. We concluded ISAs are initiated and managed inconsistently throughout DOI. From our 14 system sample, we found:

- 10 systems documented their system interconnections in the SSP and four did not;
- five of the systems completed the required documentation for an ISA and nine did not;
- four bureaus validated the required security controls were implemented by interconnected systems and 10 did not; and
- bureaus inconsistently complete ISA with other DOI bureaus, including ESN.

We determined DOI guidance was insufficient for determining when ISAs are necessary. Our sample included two systems that are part of major e-government initiatives (Recreation One Stop and Geospatial One Stop) in which DOI is the managing partner. We determined ISAs and other C&A documentation was not completed and there was no oversight by DOI over the participating partners.

Privacy Impact Assessment

OMB requires agencies to complete privacy impact assessments (PIA) and determine whether privacy information is collected and how federal agencies safeguard that information. Privacy information is known as PII and defined in OMB memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, as:

> "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

OMB memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, requires that a PIA be submitted with Exhibit 300 budget requests. In the *DOI PIA Guide,* March 2004, the Department also requires PIAs to be a component of the C&A package. DOI PIA requirements extend to all systems that contain information on individuals, including systems with information on employees and members of the public. DOI guidance requires that all systems have a preliminary review to determine if the system contains information on individuals. The preliminary review determines if the full PIA is necessary.

All 14 systems in our sample had a preliminary PIA review completed that was included in the C&A package. The PIA for eight systems in our sample stated the "systems contain information about individuals," and thus, full PIAs were completed.

We identified inconsistencies in the way PIAs for GSSs are completed and found conflicting information between some SSPs and related PIAs. The *DOI PIA Guide,* which has not been updated since 2004, states only the preliminary PIA is required if the "systems are networks that house information systems (i.e. infrastructure) … and no information is maintained in identifiable form." The guide goes further and notes PIA must be completed for each system that interfaces with the GSS. Thus, when a number of minor applications are supported by a GSS, the PIA must be completed for those minor applications to determine if those systems contain PII.

We reviewed four GSSs and found three did a preliminary PIA for the GSS level. Thus, PII potentially remains unidentified within the minor applications supported by these GSSs. One system in our sample completed the preliminary PIA for the GSS and attempted to complete PIA for the minor applications which it supported. PIAs were completed for 20 percent of the minor applications that interface with the GSS.

The SSP and PIA for Aviation Management Local Area Network (AM-LAN) presented conflicting information. The SSP stated, "Some of the AM-LAN file servers host personally identifiable information (PII)," and the PIA stated, "The system did not have PII."

We determined the DOI Privacy Intranet website, available to DOI employees, is well organized and contains comprehensive information on privacy program issues and more specifically, PIAs.

Configuration Management

In memorandum M-09-29, OMB stated, "FISMA section 3544(b)(2)(D)(iii) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Common security configurations provide a baseline level of security, reduce risk from

security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of Government information."

In March 2007, OMB directed agencies to comply with security configuration standards developed by NIST, the Department of Defense, and the Department of Homeland Security. These standards are commonly known as the Federal Desktop Core Configuration (FDCC). OMB memorandum M-08-22, *Guidance on the Federal Desktop Core Configuration*, directed agencies to meet or exceed FDCC standards regardless of the function of their workstations for the collective IT security of the government.

We conducted a computer configuration evaluation and found widespread noncompliance with mandatory FDCC standards and noncompliance with directives issued by the Department. Our testing determined the Department was 68 percent compliant with mandatory FDCC settings.

Incident Response

FISMA section 3544(a)(7) requires that agencies establish incident response capabilities and have formal procedures to detect, report, and respond to security incidents. Agencies are also required to notify and coordinate their incident response activities with the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) and notify and consult with law enforcement agencies, including their respective OIG when necessary based on the guidance. In addition, OMB memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006, requires agencies to report all incidents involving PII to US-CERT within one hour of discovering the incident.

NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, provides guidance for handling IT security incidents. The Department also has the *Interior Computer Security Incident Response Handbook*, June 2003. Many bureaus and offices have procedure guides for handling incidents within their individual organizations. We found that the documented procedures at four bureaus did not document how to report incidents to external law enforcement. For each of the 14 systems evaluated, the bureaus and offices provided complete procedures for reporting incidents internally within their organizations. Only eight of the 14 systems had procedures which included incident response for handling all forms of media involving PII. Between October 1, 2008, and August 31, 2009, DOI reported 909 incidents to US-CERT. During that same period of time, bureaus reported 1,856 incidents to DOI Computer Incident Response Center (CIRC). Of the incidents reported to DOI CIRC, 695 included requests for law enforcement assistance.

While individual bureaus and offices have documented incident response procedures, incident response capability across the Department is weak and fragmented. The Department lacks the

adequate resources to staff its own incident response capability and is unable to comprehensively monitor its network for security incidents. We determined all bureaus are using DOI's centralized reporting database (Remedy) for tracking incidents. Inconsistencies still exist, however, as to what events are reported by bureaus. During FY 2009 the Department did not facilitate incident response training.

IT Security Training and Awareness

FISMA section 3544(a)(4) requires all employees to receive annual security and privacy awareness training. The *DOI IT Security Policy Handbook* states all information system users must complete basic security awareness training before authorizing access to information systems; the *DOI IT Security Policy Handbook* does not address privacy training. FISMA section 3544(a)(3)(d) also requires the Department CIO to train personnel solely responsible for information security with respect to those responsibilities. DOI Secretarial Order 3244 delegated authority for IT career/skills management to bureau and office CIOs.

Federal Information System Security Awareness (FISSA), Records Management, and Orientation to the Privacy Act are mandatory training that must be completed annually for all employees, contractors, partners, and volunteers. An April 9, 2009 memorandum from the Department CIO to DOI Assistant Secretaries announced the requirement for Records and Privacy training and the release of both courses. Employees and contractors with major responsibilities regarding information security must complete Role-Based Security Training (RBST). In addition, all IT system users are required by Department policy and OMB memorandum M-06-15, *Safeguarding Personally Identifiable Information*, to annually acknowledge Rules of Behavior (ROB).

OMB memorandum M-09-29 states that FISMA and OMB policy (memorandum M-07-17, attachment I.A.2.d) requires that each employee receive annual security and privacy awareness training that must be included as part of the agency's training totals. During FY 2009, Department policy required all IT system users, including federal personnel and contractors, to receive annual FISSA training. In addition, bureau-level management was required to track compliance with annual training completion for both employees and contractors and was required to be 100 percent compliant by July 31, 2008. The Department was 98.4 percent compliant with FISSA training goals.

Records Management and Orientation to the Privacy Act Training

All employees, contractors, partners, and volunteers are required to annually complete both Records Management and Orientation to the Privacy Act training. Training was available and completions were tracked through the DOILearn system. Using reports from DOILearn, dated August 28, 2009, we determined the Department was 93.7 percent compliant with Records Management and 81.5 percent compliant with Orientation to the Privacy Act training.

Name of Annual Training	As of Date	Personnel completing training	Rate of Compliance (based on personnel 72,404 required)
IT Security Awareness (FISSA)	July 31, 2009	71,272	98.4 percent
Records Management	August 28, 2009	67,866	93.7 percent
Orientation to Privacy Act	August 28, 2009	59,022	81.5 percent
Total			91.2 percent

Figure 2: Completion of annual training requirements

The accuracy of training compliance rates is dependent upon an accurate determination of the number of DOI employees and other non-DOI personnel. In FY 2009, the Department determined 72,404 personnel required training. Non-DOI personnel who are also required to complete annual training includes contractors, volunteers, partners, and seasonal employees, etc. We identified discrepancies between the Department's determination of the total number of personnel and personnel counts determined using DOILearn. Bureaus generally made declarations on March 1, 2009, as to the number of employees and contractors. We identified discrepancies such as the following:

- BIA declared 2,500 contractor personnel and yet only 185 completed Privacy Act training, achieving a 7.5 percent compliance rate.

- FWS declared 552 contractor personnel, and yet only 1 person completed the Privacy Act training.

- NPS declared 18,810 personnel, and yet DOILearn reflects 20,138 personnel completed Records Management training.

- DOI states, "Interior continues to utilize the services of approximately 242,000 volunteers[7] and extensive seasonal employees;" however, bureaus and offices only included 7,217 contractors in their declaration of the number of personnel and identified no volunteers. Thus, a significant number of non-DOI personnel are not completing required annual training.

- OST declared 765 personnel on June 18, 2009, and yet only 223 completed Record Management training, which is a compliance rate of 29 percent. Their declaration included 116 contractors, and only 31 contractors were identified in DOILearn.

[7] http://www.doi.gov/budget/2010/10Hilites/overview.pdf

Role-Based Security Training

FISMA section 3544(a)(3)(d) requires the Department's CIO to train personnel with significant responsibilities for information security with respect to such responsibilities. Paragraph 1.5 of The Department's October 1, 2009 draft of *Role-Based IT Security Training Standard, Version 2.1*, defines significant IT security responsibility as any employee or contractor whose job role or function includes any of the following:

- elevated or advanced rights, beyond a general user, to DOI IT systems for IT support and administration purposes;
- bureau/office and Department officials providing IT security program management, oversight, policy, compliance, implementation, or IT security support responsibilities;
- IT managers and executives providing IT program management, oversight, policy, compliance, or implementation responsibilities; and
- other staff that have functions that impact the implementation of cyber security above their own user level.

During FY 2009, we determined 3,531 employees and contractors across the Department performed duties with significant responsibilities for information security. Bureaus and offices reported 97.2 percent compliance with mandatory RBST. Of those who completed RBST, 85 percent self-certified their training was completed. Departmental guidance permitting self-certification requires that personnel maintain artifacts to evidence the training was completed. The Department did not verify any of the self-certified training.

We reviewed artifacts to verify RBST was relevant and completed as reported. We requested copies of the documentation the Department required each self-certifying individual to maintain. After 30 days, USGS provided only a fraction of the requested data. MMS, NBC, OS, and SOL provided no data at all. Therefore, we were unable to fully review all personnel across the Department who received RBST. Our limited analysis revealed artifacts accurately supported only 15.6 percent of the self certifications. Our review further noted:

- completed courses that do not qualify as RBST, such as GovTrip, Developing Performance Standards, and Hostile Work Environment;
- incomplete or missing artifacts that failed to include hours of training, completion date, or completion certificates;

- NBC and OS stated they did not permit self-certifying for RBST and thus they did not provide any artifacts. We found, however, that 141 personnel from those organizations had completed self-certification of RBST. We determined, however, that NBC did not include those completions in their statistic for RBST completions; and

- normal operational tasks counted as RBST, for example, the BOR CIO was required to complete four hours of RBST, and BOR reported routine briefings as credit towards that requirement.

FISMA section 3544(a)(3)(D) requires that the head of each agency "delegate to the agency Chief Information Officer (CIO) (or a comparable official), the authority to ensure compliance with the requirements imposed on the agency, including . . . training and oversee personnel with significant responsibilities for information security . . ."

The DOI Role-Based Security Standard (Draft) states bureau-level management is required to enforce and track completions of RBST. DOI guidance further states in OCIO Directive 2009-005, FY 2009 *Role-Based Information Technology (IT) Security Training*, February 3, 2009, that RBST completed outside of DOILearn must be reported and tracked using the RBST self-certifying course in DOILearn. Participants completing the self-certification are responsible for retaining evidence of the external training.

User Rules of Behavior

Rules of Behavior (ROB), also called Acceptable Use Policies or standards, instruct system users, both federal and contractor, about ways in which they may or may not use IT systems. ROBs include a signature page, where the user acknowledges receipt, indicating that they understand and agree to abide by the rules of behavior. According to the DOI Policy Handbook control PL-4(a), electronic signatures are acceptable for use in acknowledging ROB. We determined multiple bureaus have users acknowledge the ROBs in Lotus Notes and in DOILearn. Such an acknowledgement is not recognized as having the same legal status as a written signature; only cryptography can provide a means of linking a document with a particular person[8]. During our inspection at FWS-Pacific Region, we determined ROBs were not signed by end users with FWS.

Identifying the population of all those required to complete training and sign ROB within DOI is an ongoing challenge. There is no reliable method to identify contractors, partners, and volunteers.

[8] NIST 800-12 section 19.2.3, Electronic signatures can use either secret key or public key cryptography; the electronic equivalent of a written signature that can be recognized as having the same legal status as a written signature

Contractor Oversight

FISMA section 3544(a)(1)(A)(ii) describes federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(B) requires each agency to provide information security "appropriate to protect such information and information systems, that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."

OMB M-09-29 requires IGs to include some contractor systems in their subset of systems and report if FISMA and other related policy requirements are implemented. The agency is required to perform oversight and evaluations to ensure information systems used or operated by a contractor of the agency, or other organization on behalf of the agency, meet the requirements of FISMA, OMB policy, NIST guidelines, national security policy, and agency policy.

DOI has 22 contractor-operated systems in their IT system inventory. We evaluated three of the systems and found two C&A packages did not clearly identify the contractor, or the contractor's roles and responsibilities, and their involvement in the C&A process. All three packages lacked sufficient detail to assess what contractor oversight was being performed by the bureau. Examples of inadequate contractor oversight included ICRs that did not document which IT security controls were assessed at the contractor facility, SSP that did not clearly distinguish controls implemented by the bureau and those implemented by the contractor, and system POA&Ms that did not evidence an exchange of information regarding IT security weaknesses.

DOI bureaus and offices use contractor support for a variety of technical services, including operations and for the management of C&A documentation. Multiple DOI bureaus and offices do not have a reliable process to identify contractors, and therefore, the bureaus and offices are unable to ensure contractors are abiding with all DOI IT security policies and procedures. There is no assurance that all contractors are complying with required security awareness training, appropriate background investigations, or non-disclosure agreements. Contractor monitoring weaknesses have been identified as a Notice of Finding and Recommendation (NFR) at FWS since 2007, at NPS since 2006, and BOR in 2009.

DOI policies do not provide sufficient guidance explaining how processes involving contractors are to be implemented. Therefore, there is no assurance that adequate contractor oversight is being performed over those who operate DOI systems or provide supporting technical services.

DOI IT Security Program

During FY 2009, information security duties consumed 14.9 percent more full-time personnel across the Department.

Information Security Personnel: FY 2008 and FY 2009 Comparison

FISMA section 3544(a)(3)(d) requires the Department's CIO to train and oversee personnel with significant responsibilities for information security with respect to such responsibilities. In FY 2009, we found more personnel fully devoted to performing significant information security duties, as well as an increase in personnel focusing more of their time on performing such duties. As in FY 2008, we again found only a fraction of these personnel performing significant information security duties under the purview of the Department CIO.

In FY 2008, the Department reported 3,343 personnel with significant responsibilities for information security. In FY 2009, the Department reported 3,531 personnel for a net increase of 188. NBC reported the largest gain in personnel with a net increase of 139. Of the 139 personnel gained, 91 were contractors. BLM reported the largest loss in personnel with a net loss of 71. Of the 71 personnel lost, 42 were employees. Figure 3, below, shows a year-by-year comparison of the total IT security personnel of DOI bureaus and offices.

Bureau	FY 2008 (FTE)	FY 2008 (CNTR)	FY 2009 (FTE)	FY 2009 (CNTR)	Difference
BIA	127	63	148	46	+4
BLM	601	123	559	94	-71
BOR	328	16	348	62	+66
FWS	284	63	275	63	-9
MMS	192	174	210	109	-47
NBC	292	141	340	232	+139
NPS	385	10	408	60	+73
OHA	5	5	6	0	-4
OHTA	5	21	5	21	-
OS	56	12	63	18	+13
OSM	37	10	39	8	-
OST	17	4	21	0	-
SOL	2	1	6	2	+5
USGS	327	42	340	48	+19
Total by Category	**2658**	**685**	**2768**	**763**	**+188**
Total by Year	**3343**		**3531**		

Figure 3: Total IT Security Personnel by Bureau, Year-by-Year Comparison

In FY 2008, the Department reported 589 personnel performed significant information security responsibilities 100 percent of the time. In FY 2009, the Department reported 677 personnel performed significant information security responsibilities 100 percent of the time, for an increase of 88 persons or 14.9 percent of the FY 2008 total. Figure 4, compares FY 2008 and FY 2009 totals of time devoted to information security duties.

Percent	FY 2008 (FTE)	FY 2008 (CNTR)	FY 2009 (FTE)	FY 2009 (CNTR)	Difference
100 percent	506	83	524	153	+88
90 or More	531	91	551	160	+89
80 or More	549	97	579	165	+98
70 or More	626	103	654	182	+107
60 or More	652	116	686	190	+108
50 or More	783	134	809	214	+106
40 or More	845	151	858	221	+83
30 or More	1027	193	1008	247	+35
20 or More	1467	329	1510	421	+135
10 or More	2058	517	2208	599	+232
9 or Less	600	168	560	164	-44

Figure 4: Percent of Time Devoted to Information Security Duties, Year-by-Year Comparison

Under-Qualified Personnel Performing Significant Information Security Duties

In our FY 2008 FISMA report, we stated, "The Department has seemingly delegated performance of significant information security duties to personnel who are likely ill-prepared to perform the task." In FY 2009, we again found many personnel reported as performing significant information security responsibilities who held positions with job titles not synonymous with information security. For example, we found a GS-15 "Pipeline Coordinator Officer," a GS-14 "Supervisory Land Law Examiner," a GS-5 "Administrative Clerk," three GS-7 "Budget Technicians," a GS-7 "Purchasing Agent," a GS-9 and a GS-13 "Contract Specialist," and a GS-7 "Personnel Specialist" were all 100 percent devoted to performing significant information security duties. In addition, we found numerous examples of seemingly unqualified people performing these duties less than 100 percent of the time. Figure 5, below, displays personnel responsible for performing significant information security duties listed by job title.

Job Title	Series	Explanation
Fish & Wildlife Biologist	0401	Provides Network And Technical Support
Wild Horse And Burro Specialist	0401	System Manager, Wild Horse and Burro System
Natural Resource Specialist	0401	Active Directory Elevated Privileges
Supervisory Natural Resource Specialist	0401	Chief Information Officer
Natural Resource Program Manager	0401	IT Help and Support
Supervisory Civil Engineer	0810	IT Project Manager
Civil Engineer	0810	Project Manager
Supervisory General Engineer	0801	Project Manager
Supervisory Hydrologist	1315	IT Security Administration
Hydrologist	1315	IT Security Administration
Geologist	1350	IT Security Administration
Supervisory Geologist	1350	IT Security Administration
Fishery Biologist	0482	IT Security Administration
Wildlife Refuge Specialist	0485	Network and Technical Support
Biologist	0482	Database Administrator
Geophysicist	1313	IT Security Administration
Cartographer	1370	IT Security Administration
Physical Scientist	1301	IT Security Administration
Supervisory Human Resources Specialist	0201	Information Resources Manager
Human Resource Assistant	0201	System Administrator
Bankcard Coordinator	0303	System Administrator
Electrical Engineer	0850	Alternate Project Manager
Realty Specialist	1170	Active Directory Elevated Privileges
Lands And Realty Supervisor	0301	Supervisor
Land Surveyor	1373	Active Directory Elevated Privileges
Park Ranger	0025	Active Directory Administrator
Director, Office Of Civil Rights	0260	System Owner
Aviation Safety Manager	0301	System Owner
Grants And Agreements	1101	Purchasing
Property Manager	1101	IT Security Administration
Secretary	0303	IT Specialist
Electronic Mechanic	2604	Local Area Network Administrator
Supervisory Budget Officer	0560	Allocate Funding
Electronics Engineer	0855	System Security Manager
Environmental Engineer	0819	IT Security Manager, System
Drug Program Coordinator	0301	Information System Security Officer
Administrative Support Assistant	0303	Part-Time IT Security
Office Aide	0303	Technical Support

Figure 5: Personnel Performing Significant Information Security Duties, by Job Title

Senior Agency Information Security Officers: Qualifications and Clearances

FISMA section 3544(a)(3)(A)(ii) requires a "senior agency information security officer" to "possess professional qualifications, including training and experience, required to administer the functions described under this section." Responsibility for "security management", however, was delegated to individual bureaus by Secretarial Order 3244, section 5(c)(2).

The *DOI IT Security Policy Handbook* states bureau and office CISOs must earn and maintain the Certified Information Systems Security Professional (CISSP) certification by International Information System Security Certification Consortium. The *DOI IT Security Policy Handbook* further requires bureau and office CISOs to hold a top-secret security clearance. We found CISOs from BIA, OST, and OHTA did not hold the required minimum professional certification. We also determined CISOs from NBC, OHTA, OSM, OST and SOL did not hold the required security clearance. Even though several bureau CISOs failed to meet the minimum qualifications defined in the Department's own policy, the Department had not identified the lack of compliance. Furthermore, these IT weaknesses were not tracked on any of the bureau POA&Ms.

Data at Rest Project

OMB directive M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006, recommends that all departments and agencies "encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing." The Department's project to implement an encryption solution for data at rest is being managed by the Department's OCIO. In our estimation, the Department is losing more than $57,000 per month in value.

The Department purchased licenses for encryption software at a cost of $691,680 for 51,397 licenses. If the licenses are not fully deployed before they expire in December 2009, the Department will have a substantial loss. Furthermore, DOI is not in compliance with OMB M-06-16, which recommended the Department "encrypt all data on mobile computers/devices which carry agency data" and further stated the Department must "ensure these safeguards have been reviewed and are in place within the next 45 days."

Non-Compliance with Guidance

FISMA section 3544(a) requires the Secretary of the Interior to delegate to the Department CIO "the authority to ensure compliance with the requirements imposed on the agency under this subchapter." Instead, we found that guidance routinely issued by the Department is not implemented. For example:

- In May 2005, the Department CIO directed all network management be transitioned to the Department by December 31, 2005. Furthermore, in November 2006, the Department

CIO directed that the Department would procure all network services and equipment. In FY 2009, we found hundreds of network circuits still operating outside the purview of the Department CIO.

- In August 2006, the Department CIO directed all bureaus and offices to transition to the Department's remote access system by January 31, 2007. In FY 2009, we found many bureaus still operating their own separate remote access systems.

- The *DOI IT Security Policy Handbook* prohibited the use of File Transfer Protocol (FTP) unless approved by the Department CIO. In FY 2009, we found many FTP servers still in use without approval.

Lack of Accuracy in DOI's IT Security Reporting

We found the bureaus and offices routinely overstated results and achievements. For example, in guidance for reporting results to the "usaspending.gov" website, the Department's guidance stated, "A score from 1-5 should be used to rate each of the below factors, then added up and divided by 5 to get the average total score. If the total score is not a whole number, round up, as we are only able to input whole numbers." Rounding up, regardless of fraction, is inconsistent with normal mathematical operations and over-inflates actual results. We also noted the Department's compliance reviews and our assessments routinely resulted in conflicting conclusions. While our reviews noted numerous errors and inconsistencies in security documentation, the Department's compliance reviews resulted in perfect, or near perfect, scores. Departmental reporting of security awareness training does not accurately reflect actual results and the reported data fails to caveat the results for assumptions. As an example, DOI does not have a reliable means to identify all contractors, partners, and volunteers required to take training, so establishing a false baseline skews the completion results.

Significant Deficiency in the DOI IT Security Program

This report provides a synopsis as to the status of IT Security within DOI. We identified governance issues, FISMA and Departmental policy noncompliance and weaknesses in oversight throughout the program. The full compilation of these findings results in a significant deficiency in the program. Thus, DOI is unable to provide reasonable assurance they are "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" information and information systems. Significant deficiency is further defined in OMB memorandum M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, August 20, 2009, as "a weakness in an agency's overall information systems security program or management control structure...In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken."

FISMA section 3544(c)(3) states agencies shall "report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2) — (A) as a material weakness in reporting under section 3512 of title 31." 31 U.S.C. section 3512 is entitled Federal Managers Financial Integrity Act (FMFIA).

Annual DOI Financial System Audit

The DOI FY 2009 Financial Statement Audit report will not be complete until November 13, 2009. As part of the audit of DOI financial systems, an assessment of Federal Information System Controls Audit Manual (FISCAM) internal controls was conducted. In addition, internal technical vulnerability assessments have been completed on the financial systems and the General Support Systems (GSS). The FISCAM requires financial statement auditors to evaluate logical access controls over financial systems to assess the level of risk associated with unauthorized access and modification of financial information.

IT Notice of Finding and Recommendations (NFRs) have been issued throughout the course of the audit for the nine bureaus. The NFR identifies weaknesses in areas such as; contractor monitoring, change control, system audit logging, Certification and Accreditation, contingency planning and multiple aspects of access control.

Internal vulnerability assessments completed at 8 bureaus identified 98 vulnerabilities which were associated with patch, password and configuration management. Of the 98 vulnerabilities, 36 were categorized as high, 52-medium and 4- low. A "Vulnerability is a flaw in the design or configuration of software that has security implications" and high, medium or low designates the potential severity level if the vulnerability was exploited.

Recommendations

To address the deficiencies identified in this report, we include many recommendations we have previously made. Until the Department addresses shortfalls in governance, it is unlikely information security will substantially improve. We recommend that the Department:

1. Realign the Department CIO to report directly to the Secretary of the Interior as required by 44 U.S.C. section 3506(a)(2)(A).

2. Realign personnel performing significant responsibilities for information security under the purview of the Department CIO.

3. Performance of significant information security duties should be consolidated and centralized to improve consistency, enhance efficiency, and reduce cost.

4. Rescind memorandum, *Information Technology Resources Management,* dated August 7, 2002, and Secretarial Order 3244.

5. Realign authority necessary to ensure compliance with FISMA under the purview of the Department CIO.

6. Realign incident response resources under the purview of the Department CIO.

7. Fully staff the incident response capability.

8. Standardize incident response tools and procedures.

9. Design and implement a standardized comprehensive and consolidated continuous monitoring program, to include continuous monitoring tools, processes, and procedures.

10. Establish and enforce minimum qualifications requirements for all personnel performing significant information security duties.

11. Implement FDCC guidelines as required by federal policy. Configurations should be standardized across the Department to improve efficiency and reduce costs. Implementation should include limiting the ability of end-users to change the configuration and the Department's ability to monitor for unauthorized changes.

12. The Department should routinely conduct testing and inspections, as well as ensure CIO guidance is fully implemented. The Department should verify POA&Ms are resolved as reported.

13. Establish and enforce standards for C&A package documentation in CSAM. Ensure consistency between the DEAR and CSAM systems.

Appendix 1: Objective, Scope, Methodology, and Related Coverage

The objective of our evaluation was to assess DOI's compliance with FISMA and to evaluate the efficiency and effectiveness of the DOI IT security program. This report reflects a compilation of the results from our evaluation of a sample of DOI information systems and other evaluations conducted by the OIG during FY 2009.

We selected a sample of DOI IT systems from the DOI IT system inventory and reviewed the C&A packages. During this evaluation, we determined if the system documentation complied with FISMA requirements and accurately reflected the security posture of the system. Our original sample included 18 systems or 8.1 percent of the IT systems from the 223 systems in the DOI inventory. Our sample included 14 systems categorized as moderate and 4 systems categorized as low. Four of the 18 systems; three moderate and one low; contained fundamental C&A issues that prevented our detailed assessment.

We considered multiple attributes and selected a sample representative of the DOI inventory. The attributes considered included: security categorization of the system, bureau ownership, OMB's high-risk list, contractor or bureau operated, application type (GSS or MA), and security application category (financial, trust, mission critical or business essential system). We eliminated four systems during our initial screening as containing foundational C&A issues, which prevented further review. The detailed assessment and our conclusions are based on the 14 systems actually assessed.

Other OIG Evaluations conducted during FY 2009 and influencing this report include:

- *Evaluation of FWS Information Technology Office-Honolulu, HI,* Report No. ISD-EV-FWS-0004-2009, June 2009. We found broad noncompliance with mandatory federal standards, as well as OMB and departmental policy.

- *Computer Configuration Evaluation*, Report No. ISD-EV-MOA-0003-2009, August 2009. We found widespread noncompliance with mandatory FDCC standards and noncompliance with directives issued by the Department's CIO.

- *Verification of FY 2007 IT Security Recommendations*, Report No. ISD-EV-MOA-0002-2009, September 2009. We found management oversight of resolving the OIG information security recommendations absent and a recent investment ("Cyber Security Assessment Management (CSAM) application") to improve information security not fully leveraged.

- *Evaluation of DOI Accountability of Desktop and Laptop Computers and their Sensitive Data*, Report No. WR-EV-MOI-0006-2008, April 2009. We found the Department as a whole could not account for the computers purchased since there is no uniform policy for the tracking and chain of custody of portable computer equipment.

- *Passport Offices Failing to Manage and Secure Employee Passports*, Report No. ER-EV-MOA-0002-2008, May 2009. We found lapses in security of diplomatic and official passports issued to employees who travel internationally on behalf of DOI.

- *FY 2008 Financial Audit Scorecard*, September 30, 2008. This report included 87 IT related NFRs for multiple DOI financial IT systems.

We conducted our evaluation in accordance with the *Quality Standards for Inspections* as put forth by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). We included tests of records and other procedures that we considered necessary under the circumstances. To accomplish our objective, we conducted the following activities:

- Reviewed applicable laws, regulations, OMB guidance, NIST standards, Government Accountability Office (GAO) reports, and Department and bureau policies

- Reviewed documentation

- Interviewed Department and bureau IT security personnel

- Performed on-site inspections of bureau and office locations

- Performed technical testing as needed to validate closed recommendations

Other Related Coverage

The OIG issued a report, *Compilation of Information Technology Challenges at the DOI*, dated May 2008, which documented the need for sweeping reform in the Department's management of information technology. To date, no significant corrective action has been taken to address the report's findings or to implement its recommendations.

Appendix 2: FISMA Fieldwork Results Summary

This matrix reflects our observations and conclusions based on review of the subset of systems across key FISMA areas. These results are used as a basis for determining DOI's compliance with FISMA. An 'X' indicates that at least one weakness was identified for the corresponding system and FISMA area.

Bureau/ Office	System Name	Acronym	System Impact Level	Certification and Accreditation	System Security Plan	Annual Self-Assessment	Risk Assessment	Incident Response	Contingency Plan and Testing	System Interconnections	PIA Process / PII Safeguards	Plan of Actions and Milestones
BIA	Eastern Zone General Support System	EZGSS	**X**		**X**	**X**		**X**	**X**			
BIA	National Irrigation Information Management System	NIIMS	**X**		**X**	**X**		**X**	**X**		**X**	
BLM	ePlanning application V. 2	eplanningV2		**X**	**X**	**X**	**X**	**X**	**X**	**X**		
BOR	Reclamation Mission Support System	RMSS			**X**			**X**				
MMS	Advanced Budget/Accounting Control and Information System (ABACIS)	ABACIS			**X**			**X**				
MMS	Outer Continental Shelf Connect	OCS-Connect		**X**	**X**	**X**	**X**	**X**	**X**	**X**		
NBC	Aviation Management Local Area Network	AM-LAN		**X**	**X**		**X**		**X**	**X**		
NBC	Financial and Business Management System (FBMS)	FBMS				**X**				**X**		
NBC	NBC Enterprise Portal (Collaborative Workspace)	NBC-EP		**X**	**X**		**X**	**X**	**X**		**X**	
NPS	NPS General Support System	One-GSS		**X**	**X**	**X**	**X**		**X**	**X**		**X**
OS	Recreation Information Database	RIDB			**X**		**X**		**X**	**X**		
OHA	OHA Network	OHANET		**X**	**X**	**X**	**X**	**X**	**X**			
OS	National Fire Plan Operations and Reporting System	NFPORS			**X**		**X**		**X**	**X**		
OSM	Abandon Mine Land Inventory System	AMLIS	**X**	**X**	**X**		**X**	**X**	**X**			**X**

Appendix 3: Security Control Analysis

FIPS 199 security categorization levels were assigned to each IT system in our sample. That designation determines the NIST SP 800-53 IT security controls that must be applied and documented in the SSP. Based on our sample of the 14 systems, we determined 89 percent of the security controls were documented in the SSP. We also determined 72 percent of the control descriptions in the SSP were adequate. We assessed the adequacy of the description by reviewing implementation descriptions and assuring the roles and responsibilities were identified. 306 IT security controls were not documented in the SSPs and 2,335 controls were documented in the 14 systems we assessed.

One system included in our original sample of 18 systems was not assessed in detail because it was classified as a low impact system, and we determined it should have been a moderate impact system. For that system, 108 security controls were not identified in the SSP. Therefore, we determined the incompleteness was too extensive to justify further review. See Figures 6, 7, and 8 below for additional details.

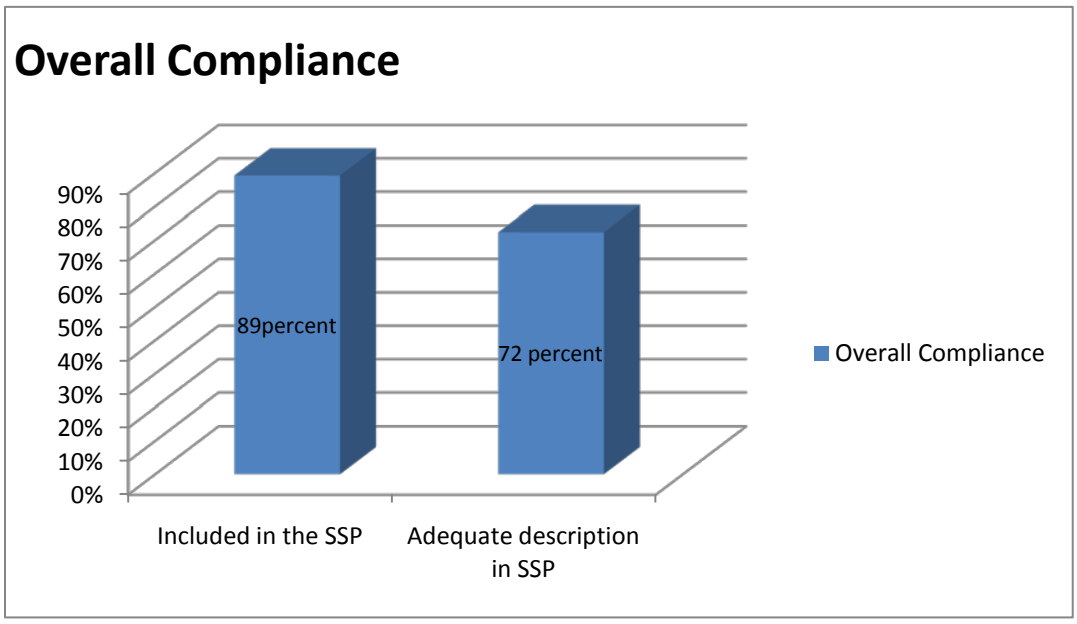

Figure 6: Security Controls documented in our system subset

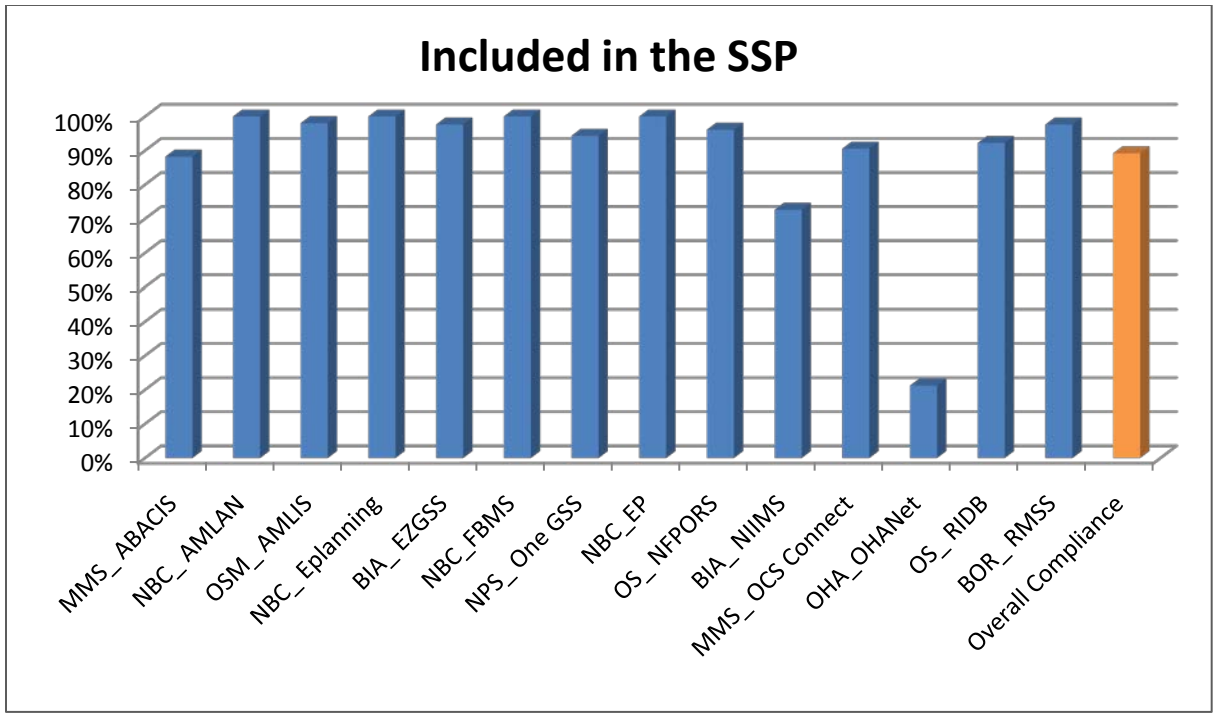

Figure 7: IT Security Controls included subset SSPs

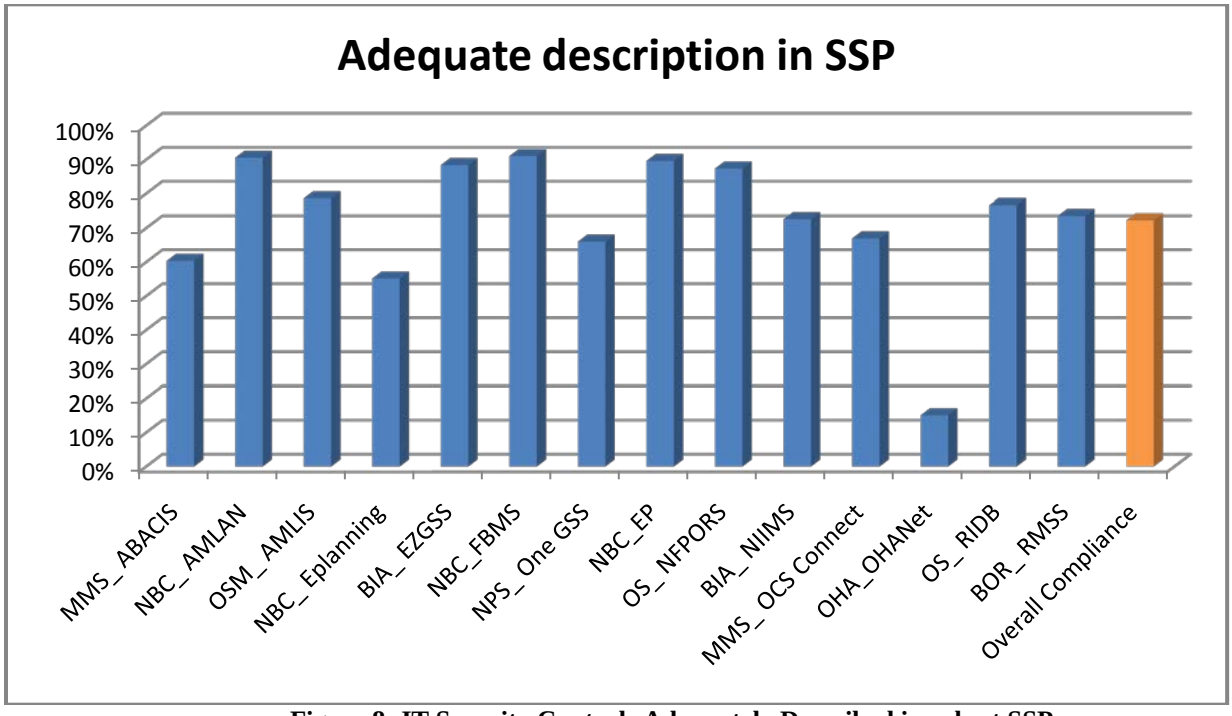

Figure 8: IT Security Controls Adequately Described in subset SSPs

Appendix 4: FISMA results between FY 2003 and FY 2008

It is estimated that DOI has expended $621.98 million on IT security since FY 2003 and yet FISMA noncompliance persists. Continuing to fund the DOI IT Security Program as it is currently structured is inconsistent with the intent of OMB A-123, *Management's Responsibility for Internal Control*, December 21, 2004, which states, "Management accountability is the expectation that managers are responsible for the quality and timeliness of program performance, increasing productivity, controlling costs and mitigating adverse aspects of agency operations, and assuring that programs are managed with integrity and in compliance with applicable law." The table below presents a summary of results included in DOI FISMA reports and the associated IT funding by fiscal year.

Fiscal Year	FISMA report conclusions	IT Budget (in Millions)
2003	"We found that the Department continues to make significant progress to improve the security over its information systems. However, its overall security program does not yet adequately protect all information systems supporting the operations and assets of the Department and therefore remains a material weakness."	The annual IT budget for FY 2003 was $791.2[9], or 5.7 percent of the DOI's overall budget($13,881)[10]
2004	"We found that the Department continues to improve the security over its information systems. However, despite sound guidance from the Office of the Chief Information Officer, we continue to identify weaknesses in bureau and office implementation of IT security requirements."	The annual IT budget for FY 2004 was $816.5 , or 5.7 percent of the DOI's overall budget ($14,325)
2005	"We have determined that there are significant weaknesses in DOI's compliance with FISMA, as well as its IT security program as a whole. Our audits, evaluations, and technical testing of DOI's systems and IT security program show that bureaus and offices are not implementing DOI policies and are not complying with OMB requirements for Certification and Accreditation."	The annual IT budget for FY 2005 was $802.8 , or 5.7 percent of the DOI's overall budget ($15,839)
2006	"Our testing and evaluation of DOI's IT Security program for Fiscal Year 2006 indicates that DOI has made good progress in the following areas: System Inventory, POA&Ms, Computer Security Incident Response, and Contractor Oversight. Still more work is needed to improve DOI's Certification & Accreditation program and the use of standard security configurations for servers, workstations, databases, and network equipment throughout DOI. Weaknesses in these two critical areas impact a broad set of federal requirements requiring the use of effective management, operational and technical controls."	The annual IT budget for FY 2006 was $934.0 million[11], or roughly 5.8 percent of DOI's overall budget ($16,122)

[9] IT Budget was estimated for FY 2003, FY 2004 and FY 2005 using the average of the FY 2006-2009 IT percentages.

[10] Total DOI Budget http://www.doi.gov/budget for each FY

[11] IT Investment Portfolio amount are from Exhibit 53 for each FY

Fiscal Year	FISMA report conclusions	IT Budget (in Millions)
2007	"DOI made good progress in a number of key FISMA areas; however, our evaluation determined the DOI information security program has not been consistently implemented throughout the Department and the resulting weaknesses hinder achievement of full compliance with FISMA."	The annual IT budget for FY 2007 was $957.6 million, or roughly 6.1 percent of DOI's overall budget ($15,799)
2008	"As in the past several years, the Department has made progress in documenting information security; however, implementation lags. There remain fundamental flaws in compliance with the FISMA. Lack of compliance is due in large part to the decentralized nature of the Department , IT program and lack of authority by the Department's CIO. These serious organizational flaws potentially negate the many millions of dollars spent on IT security annually. Lack of departmental oversight, coupled with questionably qualified personnel performing information security duties across the Department, contributes inadequate incident detection and response capabilities put the Department at substantial risk."	The annual IT budget for FY 2008 was $952.7 million, or roughly 5.4 percent of DOI's overall budget ($17,475)
2009	"As in previous years, we found DOI does not fully comply with the FISMA. The decentralized organizational structure, fragmented governance processes related to the IT program, lack of oversight, bureau resistance to departmental guidance, and use of substantially under-qualified personnel to perform significant information security duties exasperates the challenges in securing the Department's information and information systems."	The annual IT budget for FY 2009 was $965 million, or roughly 5.6 percent of DOI's overall budget ($17,183)
Total IT Spending FY 2003-09		Roughly $6.2 billion has been expended for the DOI IT program
IT Security Spending FY 2003-09	Conservative Assumption: IT Security 10 percent of IT Budget	Estimate $621.98 million has been expended for IT Security between FY 2003 and FY 2009
2010		Proposed annual IT budget for FY 2010 is $996 million or 8.2 percent of the DOI overall budget

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 4428 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 06/08