EVALUATION

OFFICE OF
INSPECTOR GENERAL
U.S.DEPARTMENT OF THE INTERIOR

FY 2010 FISMA
EVALUATION REPORT

Report No.: ISD-EV-MOA-0001-2010

November 2010

Table of Contents

Results in Brief

Our fiscal year (FY) 2010 FISMA Evaluation Report reveals major inconsistencies in the U.S. Department of the Interior's (DOI) Information Technology (IT) security program. These inconsistencies are a reflection of DOI's decentralized approach to governing IT security. Each bureau manages its own security program, as the Department Chief Information Officer does not have the authority to unify and align the Department's IT security program.

We found several DOI systems missing or not clearly identified in inventory databases, and that potentially helpful investments were sitting idle on shelves. We also identified key program areas that are not consistently implemented, such as incident response, configuration management, and remote access.

- Our unannounced tests of DOI's incident response capabilities revealed that social engineering gained us network access and access to sensitive information following requests to reset the passwords of key personnel. We found that these potential security breaches occur without being identified and fragmented reporting processes enable these events to continue.
- Our testing revealed that bureaus have installed multiple Web browsers that are not compliant with the Federal Desktop Core Configuration standards.
- We determined that DOI bureaus continue to use multiple remote access solutions to which the Department has no insight. We identified one of these remote solutions, which the Department did not know that the bureau had implemented. The bureau was forced to shut it down until it could be formally documented and risks assessed.

We found that the information that authorizing officials use as the basis for their operating decisions is incomplete and inaccurate. This information, which comes to them in a package containing the system security plan, security assessment reports, and plans of action and milestones, should be complete enough for an authorizing official to assess the risks of operating a system. More than half the packages we found were incomplete or lacked the necessary quality to provide authorizing officials with an accurate view of the system security posture. This inadequacy presents further challenges for the Department as it prepares to meet new National Institute of Standards and Technology requirements to move this process toward ongoing security authorizations.

We also found promising programs in DOI's IT security. One such program requires that all DOI employees and contractors use a personal identity verification card to log into the network. This will significantly increase network and remote access security. To date, 76 percent of employees and 23 percent of contractors are enrolled.

Also, the Department launched the DOI Innovation and Efficiency Team (DIET) Initiatives in June 2010. Although DIET is still in the planning stages, this initiative promises to provide long-term solutions to cost efficiency.

Introduction

Increased cyber threats have resulted in the establishment of security standards meant to unify the Federal Information Security Management Act (FISMA) framework for the Federal Government.

Fiscal year (FY) 2010 has seen the greatest changes to FISMA requirements since its inception in 2002. The U.S. Department of the Interior (DOI or Department) have not managed to keep pace. Weaknesses in fundamental areas of the Department's Information Technology (IT) security program remain unresolved.

Objective

This report summarizes the results of our FY 2010 FISMA Evaluation of the Department's IT security program. We evaluated DOI's compliance with the requirements of the Federal Information Security Management Act and related information security policies, procedures, standards, and guidelines. This report also contains recommendations to enhance DOI's information security program and move toward full FISMA compliance.

Background

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

FISMA also requires the Secretary of Commerce to prescribe compulsory, binding standards and guidelines pertaining to Federal information systems. As a component of the Department of Commerce, the National Institute of Standards and Technology (NIST) is required to develop Federal Information Processing Standards, which define the minimum requirements for information security and system security categorizations. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems. NIST introduced two publications in the last year that have significantly changed Federal agency information security programs. The revised guidance includes:

- NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems;" and
- NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."

These publications updated IT security controls to address cyber threats, emphasize IT risk management and continuous monitoring, and recognize that authorizing officials need to have access to near real-time monitoring. Compliance with FISMA is no longer dependent upon a stagnant certification and accreditation package, rather the requirements have moved toward ongoing information system authorizations.

The Office of Management and Budget (OMB) must report annually to Congress on all Federal agencies' FISMA compliance. OMB used CyberScope as the automated FISMA data collection instrument for reporting on agency compliance. CyberScope contained 11 areas for OIG input in FY 2010:

- Certification and Accreditation Program;
- Status of Security Configuration Management;
- Status of Incident Response and Reporting Program;
- Status of Security Training Program;
- Status of Plans of Action and Milestones Program;
- Status of Remote Access Program;
- Status of Account and Identity Management Program;
- Status of Continuous Monitoring Program;
- Status of Contingency Planning Program;
- Status of Agency Program to Oversee Contractor Systems; and
- Financial Audit.

Enterprise Initiative

The Department launched the DOI Innovation and Efficiency Team (DIET) Initiatives in June 2010 "to identify and implement immediate and long-term solutions to realize cost savings, cost avoidance, cost efficiencies and/or innovations across the DOI IT environment." DIET, which is still in the planning phase, includes objectives and projects that, once implemented, promise to contribute to the IT Security Program.

The DIET Initiatives include:

- Infrastructure consolidation (of facilities, telecom, servers and storage, applications and data, and IT asset inventory);
- Data center consolidation;
- Unified messaging;
- Risk-based Information Security Services;
- Radio site consolidation; and
- Workstation ratio reduction.

Findings

The findings in this evaluation are organized by the 11 Information Technology (IT) security program areas: IT inventory, certification and accreditation, security configuration management, incident response and reporting, security training, plans of action and milestones, remote access, account and identity management, continuous monitoring, contingency planning, and oversight of contractor systems.

We also include all relevant policies, guidance, requirements, regulations, or definitions and answer whether or not the Department's bureaus follow that existing guidance.

IT Inventory

Policy

The U.S. Department of the Interior (DOI or Department) has established a policy for maintaining IT inventory, but confusion over the policy has impacted its accuracy. Managing the DOI IT infrastructure is dependent upon an accurate inventory and provides a foundation for an effective IT security program and FISMA compliance.

The March 2008 DOI IT Security Policy Handbook (Version 3.1), requires bureaus to "track all IT system components and security status by maintaining a comprehensive inventory in the DOI Enterprise Architecture Repository (DEAR)." The Chief Information Officer (CIO) issued a directive[1] establishing DEAR "as the official data source for DOI enterprise architecture artifacts, [and] all DOI information systems." The directive also states that the bureau CIOs are responsible for annual written assurance that data in DEAR is accurate and complete.

DOI also implemented the Cyber Security Assessment Management (CSAM) solution, which identifies IT system inventory. Its primary purpose, however, is to be the official repository for preserving Certification & Accreditation (C&A) Package documentation, Plans of Action and Milestones (POAM), and Internal Control Reviews for each system in inventory. A September 23, 2008 Departmental memorandum, titled "Mandatory Use of the Cyber Security Assessment Management (CSAM) Solution" and signed by the Acting Department CIO, specifies mandatory use and full implementation of the CSAM solution.

On April 27, 2009, we issued a management advisory, "Deficiencies in System Inventory Management," which states that disparities exist between DEAR inventory and the inventory documented in C&A packages. The Department CIO

[1] Office of the Chief Information Officer Directive No. 2009-002, "Population and Maintenance of the Departmental Enterprise Architecture Repository," February 6, 2009.

responded to the management advisory on July 9, 2009, stating corrective action was taken for the discrepancies. The Department also stated that it had “initiated a more robust data harmonization effort.” We determined corrective actions were not focused on the systemic process weakness. We identified similar issues in FY 2010.

Our review identified that inaccurate and incomplete system inventory is unreliable for identifying accreditation boundaries. We also found that bureau CIOs are not certifying inventory as policy requires.

System Inventory

DOI has not established clear procedures to consistently manage its IT inventory, which results in confusion among bureaus as to which system is used for maintaining inventory.

During our fieldwork, three bureaus stated that CSAM is the most accurate source of inventory information, but the Department has documented and confirmed that DEAR is the primary system for maintaining IT inventory. Despite weekly data feeds from CSAM to DEAR, the two systems are not reflective of each other and they maintain different data elements.

National Institute of Standards and Technology (NIST) Special Publication 800-37 defines an accreditation boundary[2] as “all components of an information system to be accredited by an authorizing official.” DEAR is used to maintain the Department’s accredited IT system inventory and component parts, but bureaus maintain the inventory of component parts inconsistently. DEAR does not present an accurate view of the accreditation boundary and the components, accounting for 253[3] accredited systems (which include placeholders for pending and unmatched), while CSAM reflects 270. The component under each accredited system is not identified in inventory.

The bureaus use a wide, and often confusing, array of terms related to inventory management. The Department also has no organization-wide agreement for the definition of “systems,” and bureaus use inconsistent criteria when determining how all identifiers are used to manage IT inventory.

Sample of Systems reveal Inventory Discrepancies

Inventory entries into DEAR and CSAM are neither complete nor managed consistently across the Department. Our sample of systems showed:

- Inconsistent identification of inventory
  - The Talent Management System was not included in DEAR inventory and was only entered in CSAM as a minor application

[2] NIST Special Publication 800-37, Revision 1, states that the term “accreditation boundary” is synonymous with “information system boundary” and “authorization boundary.”
[3] Based on the “DEAR Certification & Accreditation Boundaries-All C&A Detail” July 13, 2010 report.

    with the Human Resource Management Suite accreditation boundary following our request for documentation. This is not the National Business Center's (NBC) normal process. The Talent Management System is now the only minor application in NBC's system inventory in CSAM;
  - DOI has consistently failed to include development systems, such as the Incident Management Analysis and Reporting System, which has been in development since 2004, in inventory. It was added into DEAR and CSAM only after we included this system in our sample;
  - The Radio Program General Support System is not in DEAR or CSAM inventory; and
  - The Project Portfolio System is not in DEAR or CSAM inventory.
- Incomplete inventory
  - The National Park Service General Support System (OneGSS) has significant minor applications, such as the Concession Management System, which is not identified with its accreditation boundary in DEAR inventory;
  - The Native American Student Information System does not have any components associated with the system in DEAR inventory, yet a contractor operates a portion of the system;
  - The National Conservation Training Center Local Area Network does not have any minor applications, yet a contractor operates an associated property management system; and
  - The Science and Support System-Low (S&SS-Low) was one of the systems receiving minor applications from two retired U.S. Geological Service (USGS) systems, yet the minor applications are not identifiable in DEAR or CSAM inventory and associated with S&SS Low.
- Sites with no minor applications
  - The Bureau of Land Management (BLM) General Support System (GSS) state, district, and local offices are in DEAR and CSAM inventory with no minor applications; and
  - NPS OneGSS parks, offices, and centers are in CSAM inventory with no minor applications.
- Minor applications with no sites
  - Office of Surface Mining (OSM) GSS minor applications are in DEAR and CSAM inventory and the security documentation agrees; and
  - Office of the Special Trustee (OST) NET minor applications are in CSAM inventory, but the security documentation does not agree with inventory.

Inaccurate Inventory used for Management Decisions

Management decisions based on incomplete and inaccurate inventory introduce risks to the IT security program. It is not prudent for an authorizing official to operate a system and assume the risk without a clear understanding and accurate documentation of all components included in the accreditation boundary. Furthermore, each year the bureau CIOs are required to certify that their bureau's DEAR database — an inventory system that is not consistently managed and documented — is accurate and complete. In FY 2010, five bureau CIOs completed DEAR certifications, including U.S. Fish and Wildlife Service (FWS), Minerals Management Service (MMS), NBC, NPS, and Office of Historical Trust Accounting (OHTA). We reviewed the completeness of DEAR inventory for the five bureaus that completed the CIO certification and determined only the MMS system, is in fact accurate and complete.

Accreditation Boundaries

An accreditation boundary identifies the information resources covered by the authorization decision. NIST Special Publication 800-37, Revision 1, changes the term "accreditation boundary" to "authorization boundary" or "information system boundary." The authorization boundary is "the set of information resources allocated to an information system" and "well defined boundaries establish the scope of protection for organizational information systems."

Authorization boundaries are poorly defined and documented throughout much of the Department. Errors and omissions in the DEAR system inventory amplify boundary discrepancies and vague definitions. DEAR, CSAM, and the authorization package do not provide an accurate view of system authorization boundaries. Authorizing officials make decisions to operate systems based on the boundary described in the authorization package and in DEAR inventory. The risks associated with the system are not identifiable if boundaries are not accurately identified.

Contractor Systems

DOI guidance is unclear as to when IT systems or subsystems should be identified as a contractor system in inventory. NIST Special Publication 800-37, Revision 1, defines a Federal information system as "an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency." Contractor systems are to be identified in IT inventory separate from agency-owned systems, but DOI guidance does not specify further criteria for determining if contractor systems or subsystems should be identified in DEAR.

Bureaus do not consistently identify contractor systems inventory. Our sample of systems revealed that the identification of contractor systems is inconsistent when both agency and contractor share in hosting or operations.

Two systems in our sample were identified as contractor systems in inventory. Those systems include:

- The Land Records Information System, which is hosted in a DOI Government facility. The system security plan does not reference contract operators; and
- The OHTA Clifton Gunderson Indian Trust Information System, which is hosted at a contractor facility and operated by contractors.

Three other systems in our sample are fully or partially hosted or operated by contractors and are not identified as contractor systems, including:

- The DOI Enterprise Services Network, which is hosted in a Government facility and primarily operated by contractors, along with some Federal personnel;
- The Native American Student Information System, which is primarily hosted in a Government building in Albuquerque, NM, and partially at a contractor facility in Blaine, MN, where contractors provide system administration and help desk support; and
- The National Conservation Training Center Local Area Network hosted at a Government building and includes a Property Management System that is managed by a guest services contractor.

Not clearly identifying contractor systems has impacts beyond the IT inventory. Authorizing officials receive incomplete descriptions of the systems via the C&A packages, DOI cannot oversee contractors and assure compliance with FISMA security requirements, and contractor data centers are not accurately identified, which causes them to be left out for consideration in the Department's data center consolidation efforts.

Hardware and Software Inventory

Conditions at DOI present persistent challenges to maintaining a valid asset inventory. IT acquisitions for hardware and software are not centralized at all bureaus and controlling what is deployed on the network is difficult. Network access controls are not implemented throughout most of DOI, which means there is not an effective way to control what hardware connects to the network. In addition, the widespread use of local administrator rights enables users to install unauthorized software.

The "Department's C&A Guide Using CSAM" states that asset inventory includes "all hardware and software, including Servers, Workstations, O/S [operating system], software suites, applications, Web functionality, development applications, virus protection, Web tools such as Cold Fusion, VPNs [Virtual Private Network], encryption tool, firmware, modems, hubs, routers, contractor authorized hardware and software, firewalls, IDS [intrusion detection system], scan tools, etc."

The Department has the technical capabilities to identify IT asset inventory, but bureaus impose limitations on the network, which prevents DOI insight into all bureaus. As a result, asset inventory is not centrally managed and bureaus do not use consistent methods to identify their asset inventories. Some bureaus use automated mechanisms to generate asset inventory reports while other bureaus have a manual process, and one bureau is unable to report.

Recommendations

1. Standardize the use of terms within CSAM.

2. Establish clear guidance for managing IT assets system inventory, including: the identification and documentation of minor applications, the identification (description, hosted, or operated) and documentation of contractor components, a process for adding systems in development to inventory, a process for adding test systems into inventory, and a process for mapping all components to authorization boundaries.

3. Establish clear guidance for managing hardware and software asset inventory.

Certification and Accreditation

Policy

System accreditation is required by the Office of Management and Budget[4] and is a required FISMA process. Accrediting an information system means a "senior 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," according to the Department's June 2009 "C&A Guide Using CSAM Solution" (Version 2.0). The C&A process documents the system security requirements, security controls, and authorization to operate the system.

In February 2010, NIST issued revised guidance[5] that transforms the traditional C&A process into a six-step Risk Management Framework, now known as the "security authorization process." In addition, August 2009 guidance[6] modified the required minimum IT security controls for systems. DOI has yet to update its C&A policy to correlate with NIST's revised guidance.

The C&A policies detailed in the DOI IT Security Policy Handbook are based on the traditional C&A processes, now outdated by NIST's February 2010 and August 2009 guidance. The Department also has multiple procedural documents for implementing the C&A process, including the draft "DOI Certification and

[4] Circular A-130, Appendix III.
[5] NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems."
[6] NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."

Accreditation Guide" (February 4, 2008) and the "DOI C&A Guide using CSAM Solution."

We found that bureaus were aware of the various policy and guidance documents, yet do not have a definitive understanding of which guidance to follow. Confusion over the policy and procedural guidance has impacted the implementation of DOI's C&A program.

FISMA Sample of Systems

The weaknesses we identified in our sample are indicative of a flawed Departmental authorization process. Such issues adversely affect the authorizing official's capability to manage information security system risks. Our review determined most of the C&A packages would not give an authorizing official a comprehensive and valid understanding of the system security posture and could not be relied on to support their decision to authorize the operation of the system.

We reviewed a representative sample of 21 IT systems to assess the Department's C&A process (See Appendix 1: Scope and Methodology for the complete list of systems). Our review revealed noncompliance with DOI procedures, documentation deficiencies, invalid accreditations, complex systems not identifying and describing component parts, untimely updates of system security plans, and self assessment of controls and contingency plans.

Our review was based on data provided by bureaus and artifacts from CSAM. CSAM is the official repository for C&A packages, POAM, and Internal Control Reviews for each accredited system in inventory.

CSAM experienced a system failure and backup glitch that had a major impact on the completeness and accuracy of the data in CSAM. The Department CIO stated on July 2, 2010, "Unfortunately, analysis has revealed a breakdown in database backup processes and procedures resulting in loss of data entered into CSAM since approximately February 19, 2010." Since our FY 2010 FIMSA Evaluation was underway during that time, some of our findings may have been impacted. Commonalities we identified in the sample of systems included weaknesses in documentation, system accreditation, control reviews, and contingency plan tests.

Documentation

We found that C&A documentation is done inconsistently and lacks quality. We assessed the C&A packages for our systems sample and determined an overall quality rating of "good," "satisfactory," or "poor." The ratings were based on sufficiency and completeness of detail within the package, compliance with NIST and Departmental guidance, and document organization. Our primary focus was to see if the package provided an authorizing official with an accurate understanding of the system security posture to make valid decisions to operate the system. We found security documentation that showed 62 percent of the 21 systems were in the “poor” category, 24 percent were “satisfactory,” and only 14 percent were “good.”

Some C&A packages were generated using the CSAM system capabilities, while others were produced independently. The packages generated using CSAM generally lacked tailoring and system-specific detail. CSAM is capable of generating a complete authorization package, but the end result is only as good as the original data entered. We found that portions of the system security plans were missing information and only displayed templates or placeholders. We also identified system security plans with broken hyperlinks, generic responses, limited or no documented update history, and blank signature pages for system security plan approval. Packages produced independently of CSAM were found to be more complete and the documents were reviewed for quality.

System Accreditation

During our evaluation of the FISMA sample of systems, we indentified varying issues with system accreditation. We noticed several weaknesses with the documentation and the process. Problems include:

- Not all systems are accredited;
- The accreditation process for systems in development is unclear;
- Component parts are not fully identified within a larger accreditation boundary; and
- Not all accreditations are completed on time. Furthermore, minimum controls have not been implemented following NIST revisions in August 2009.

Accreditation Problems and Weaknesses

First, not all Department systems are accredited. We identified three systems (Radio, Project Portfolio Management, and S&SS-Low) that are deployed in the DOI environment to varying extents and determined that they are neither covered under valid security authorizations, nor fully identifiable in the DEAR IT inventory.

The Radio Systems Program accreditation has not been completed to date. Radio systems are used in various missions by the Bureau of Indian Affairs (BIA), BLM, FWS, NPS, Bureau of Reclamation (USBR), and USGS. Since the DOI Radio System Program was one of the systems in our sample, we requested security documentation on December 17, 2009, and were informed the consolidated program or bureaus’ instances do not have supporting C&A packages. The Office of Management and Budget classifies radio systems as a General Support System, and they must adhere to FISMA requirements, including system accreditation. DOI established the Radio Site Consolidation project charter on June 18, 2010, to analyze alternatives and the feasibility of restructuring the program, but accreditation has not been completed.

Project Portfolio Management does not have a valid accreditation. The system is used by the DOI investment review board and is not included in DEAR inventory or CSAM. We did not receive a response from the Office of the Secretary (OS) regarding our request for system documentation.

The Science and Support System-Low (S&SS-Low) accreditation has not been completed. During our FY 2009 FISMA evaluation, we expressed concerns about the accreditations of two USGS systems: the Office Automation General and Office Automation Specialized. The Associate Director for Geospatial Information and CIO stated on June 12, 2009, that "in accordance with the boundary change certificate memo, the subject systems will have all Assets or constituent subsystem-level components realigned into new systems, therefore decommissioning the old systems is required." Our FY 2010 sample included two systems (S&SS-Low and S&SS-Moderate) on the receiving end of this USGS component realignment. We are unable to reconcile the asset realignment and gain assurance that all component systems are properly accredited for this evaluation.

Second, the Department's guidance regarding the accreditation process for systems in development is unclear. The Department's C&A Guide elaborates on the Clinger-Cohen Act, which "directs the heads of agencies to '*incorporate information security principles and practices throughout the lifecycles of the agency's information systems*,'" by stating, "Therefore, any automated information resource under development, and at any stage during operation and maintenance through disposal, must be included in the security requirements of the system."

We included one such system in our sample to gain an understanding of how the authorization process is implemented during system development. We found that the system, Incident Management and Analysis and Reporting System (IMARS), which is being created to provide a Department-wide information collection, analysis, and reporting system for law enforcement and non-law enforcement, lacks proper documentation and does not have a timely accreditation process underway.[7] The system has been in various stages of development since 2004 but the security documentation process has not moved forward. IMARS is on the Office of Management and Budget's FY 2010 high risk information technology projects list. The necessary security considerations have not been documented.

When we requested the C&A package for the IMARS system, we received a memorandum from the authorizing official with a brief status update, which did not detail the NIST defined tasks that should be underway. Also, the

[7] NIST Special Publication 800-37, Revision 1 (page 5), describes the process for managing information systems-related risks, including, "integrating information security requirements into system development life cycle." Many of the tasks associated with the system's authorization process are detailed in NIST 800-37 and begin during system development.

Department's official repository for C&A package documentation, CSAM, does not contain any security-related documentation for the system.

Third, we found that component parts are not fully and consistently identified within a larger accreditation boundary. When we looked at component parts, or minor applications within complex systems, to determine if they are adequately identified in the accreditation package, we found that the level of detail varied by system size and by bureau.

As an example, inconsistencies were identified between bureaus in how they reflect components in CSAM. The Office of the Secretary successfully and effectively identified the component part (the Talent Management System) within the Human Resource Management Suite major application package. We determined that NPS did not adequately describe the two applications we reviewed. The Yosemite Wilderness Permit System and the Concession Management System were neither described in detail nor clearly identified in the related GSS accreditation package.

Also, despite guidance from the CSAM C&A Guide, the Concession Management System minor application is not fully identifiable in DEAR and associated with the NPS OneGSS. Both NPS minor applications are not fully described in the system security plan, security categorization is not documented, and the security controls are not identified for each subsystem component.

Finally, we found reaccreditations that were not completed in a timely manner. NIST states that the maximum authorization period for an information system is 3 years. Four sample systems had accreditations that expired during our evaluation. The reaccreditations were not completed to correspond with the accreditation expiration date. In all instances, the reaccreditations were between 60 and 90 days overdue, as of the date of this report. One date reflected in CSAM showed that the accreditation expired on June 11, 2011, but the signed accreditation memo shows that the accreditation expired on August 7, 2010.

Annual Self Assessments and NIST Revisions

FISMA § 3544(b)(5), requires annual assessments of the effectiveness of information security policies, procedures, practices, and security controls for all systems. The CIO issued a memorandum[8] with detailed instructions and a methodology for completing annual self-assessments for systems. It included a requirement that CSAM should be used to document all system Internal Control Review assessments for FY 2010. We found that only 67 percent of the bureaus are using CSAM to assess the system IT security controls.

NIST Special Publication 800-53, Revision 3 guidance has not been addressed in DOI guidance. All controls in that guidance have not been implemented. Most C&A packages are based on the second revision (NIST Special Publication 800-

[8] "Internal Control Review Guidance for FY2010," February 24, 2010.

53, Revision 2), instead of the current version, which was released in August 2009. These updates were to be fully implemented by August 2010, but CSAM has not yet been updated. The FY 2010 annual assessments were completed using Revision 2, but the additional controls have not been assessed, and we have no assurance all minimum baseline controls have been implemented.

Also, we identified multiple process weaknesses during our review of self assessments. We did not find a historical record of assessments consistently posted in CSAM, so we were unable to ascertain if all systems had undergone an annual assessment within 12 months of their FY 2009 self assessment. We also found that large and complex systems do not have a methodology to effectively consolidate control assessments when they are completed at multiple sites under the accreditation boundary. Many security controls did not contain any implementation description.

Contingency Plan Testing

We found inadequate contingency plan testing within the Department. Our sample revealed that 67 percent of the system contingency plan tests were either not completed on time or were insufficiently documented. The DOI IT Security Policy Handbook states that bureaus must test the contingency plan for information systems “at least annually using bureau or office developed-tests and exercises to determine the plan’s effectiveness and the organization’s readiness to execute the plan.” We found multiple systems had test date data entered in CSAM, but no artifacts were provided to support the entry. Without comprehensive and well-documented contingency plan tests, DOI is unable to have confidence in their plans.

DOI Compliance Reviews

We found an ineffective compliance review process within the Department. The results from the reviews are often inflated and they are of little benefit to the bureaus.

The Department’s Cyber Security Division conducts annual reviews at each bureau as part of the Department’s FISMA oversight and compliance efforts. There is overlap between the OIG FISMA Evaluation and Cyber Security Division’s compliance reviews; however, the OIG and Cyber Security Division results often disagree.

Our evaluation noted numerous errors and inconsistencies in the bureaus’ authorization packages, yet the Cyber Security Division’s compliance reviews resulted in perfect, or near perfect, scores. During our fieldwork, bureaus expressed confusion over the differences in our findings and Cyber Security Division’s lack thereof. Bureaus further stated that the Cyber Security Division gave them an opportunity to correct identified deficiencies and have their score modified.

Recommendations

4. Update DOI's security authorization policy and guidance to incorporate the latest NIST guidance (NIST 800-37, Revision 1, and NIST 800-53, Revision 3).

5. Merge the multiple DOI security authorization procedural documents into a single document. The guidance should clarify when the authorization process begins in the life cycle, the role of the senior risk executive, and clarify how information system boundaries are to be documented.

Security Configuration Management

Policy

Security configuration management is fundamental to the overall success of an information security program. FISMA emphasizes the need for organizations to implement an organization-wide information security program. A March 22, 2007 Office of Management and Budget memorandum directed agencies to comply with Federal Desktop Core Configuration (FDCC) standards, the security configuration standards that were developed by NIST, the Department of Defense, and the Department of Homeland Security, by February 1, 2008. One year after OMB's memorandum, the Department's Office of the Chief Information Officer issued policy in March 2008 requiring all offices to be in full compliance with FDCC standards by September 30, 2008.

Federal Desktop Core Configuration

FDCC standardizes desktop and laptop configurations and is intended to provide a secure, enterprise-wide managed environment. Departmental policies require compliance with FDCC and also that deviations are documented and approved.

We performed technical testing and assessed FDCC compliance by measuring specific standards and configurations settings on the following benchmarks: [9]

- Windows XP Professional;
- Internet Explorer Version 7; and
- Windows XP Firewall.

We found that the Department was 80 percent compliant[10] with FDCC benchmarks in 2010, compared to 68 percent compliant in 2009.We also found inconsistencies, however, such as disparate Web browsers, and unapproved

[9] We assessed compliance with FDCC where bureaus had these three benchmarks available. Not all bureaus employed these benchmarks, so we were unable to test disparate software.

[10] OIG Secure Content Automation Protocol (SCAP) testing did not take into account approved or unapproved deviations.

FDCC deviations. We reviewed the concept of least privilege and its implementation and impact on security configuration management. The inconsistent configurations present a challenge in securing DOI workstations and hinder the Department's ability to monitor FDCC compliance.

We conducted technical testing in June 2010 and found FDCC compliance varies by bureau as demonstrated in Figure 1. We tested all bureaus with the exception of OHA, as technical testing capabilities were not available to test their operating systems. We found differences in FDCC compliance ranging from 58 to 95 percent throughout the bureaus.

Overall Percentage of Compliance with all FDCC Benchmarks

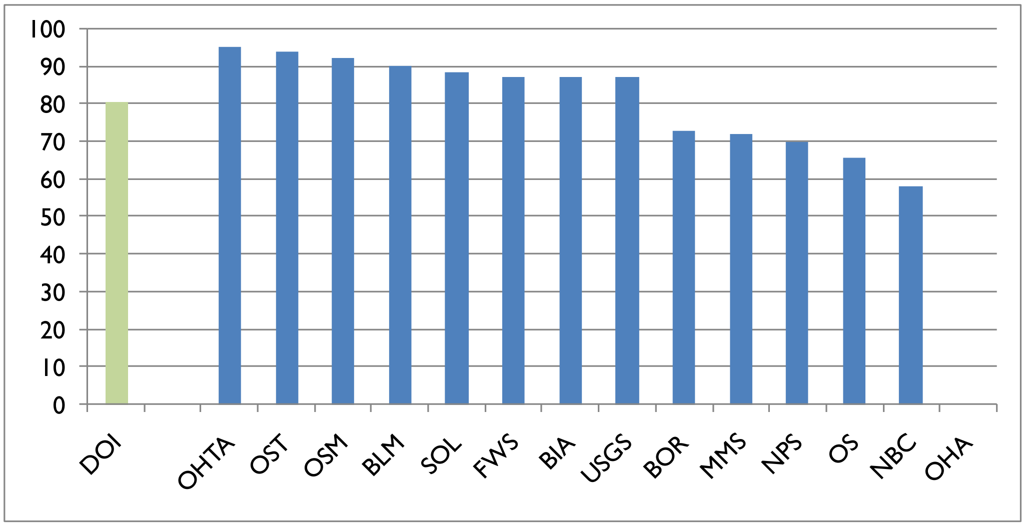


Figure 1. We found differences in FDCC compliance ranging from 58 to 95 percent throughout the bureaus.

Inconsistencies

We identified inconsistencies and unapproved deviations throughout much of the Department during our data analysis. These inconsistencies make monitoring the Department's overall FDCC compliance challenging. We found that:

- BIA, USBR, MMS, and OSM were unable to validate their own compliance with FDCC;
- BLM, FWS, NPS, OHTA, OST, and SOL did not have approved deviations from mandatory FDCC settings;
- MMS, NBC, NPS, Office of the Secretary (OS), and OST do not use the inherent Windows XP firewall, which puts them at risk for not meeting FDCC security requirements;
- USBR, FWS, and USGS do not have firewalls consistently turned on like other bureaus;

- One typical Office of the Secretary user with elevated privileges managed his own FDCC compliance settings instead of receiving the Department's policy through automated mechanisms; and
- One Office of the Secretary user did not have a firewall turned on at any time.

Disparate Web Browsers

We found multiple versions of Web browsers throughout the agency. FDCC mandates that each browser be configured with equivalent FDCC settings, yet we found BIA, BLM, USBR, FWS, MMS, NBC, OS, OSM, and USGS did not configure their additional browsers to be secure. The following table demonstrates the Department's disparate Web browsers:

Disparate Web Browsers by Bureau

Bureau	No. of Browsers Reported	Browsers and Versions Identified
BIA	5	Internet Explorer 7 and Internet Explorer 8; Multiple versions of Mozilla Firefox; Multiple versions of Safari; Netscape Navigator; and Google Chrome
USBR	5	Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8; Multiple versions of Mozilla Firefox; Multiple versions of Safari; Google Chrome versions 1-5; and Opera V9 and V10
BLM	2	Internet Explorer 7 and Mozilla Firefox
FWS	5	Internet Explorer 7 (FWS did not identify the other 4 browsers)
MMS	2	Internet Explorer and multiple versions of Mozilla Firefox
NBC	2	Internet Explorer and Mozilla Firefox
NPS	5	Internet Explorer 7 and Internet Explorer 8; Multiple versions of Mozilla Firefox; Netscape Navigator; Google Chrome; and Opera
OHA	2	Internet Explorer 7 and Internet Explorer 8
OHTA	0	0
OS	2	Internet Explorer and Mozilla Firefox
OSM	2	Internet Explorer and Mozilla Firefox
OST	0	0
SOL	0	0
USGS	5	Internet Explorer, Mozilla Firefox, Safari, Google Chrome, and Opera

Figure 2. These are the browsers that each of the bureaus reported in the OIG data call. In some cases, the number of browsers reported differs from the number actually identified.

Least Privilege and Elevated Rights

FDCC standards prohibit elevated privileges and require least privilege for users, a concept in which users are assigned the absolute minimum privilege necessary to perform required tasks (e.g., "local administrator" or "power user" settings). Assigning elevated privileges, such as "local administrator" or "power user," enable users to circumvent standard configuration controls. According to NIST, any privilege that is not a default user right is an "escalated privilege" and is not in compliance with FDCC.

We found six bureaus that elevated “typical” or “normal” user accounts to “local administrator” or “power users.” Moreover, these users are constantly logged in with escalated rights and privileges, thus inviting the opportunity for malicious software (malware) that can damage Department files and settings.

Percentage of Users with Local Administrative Privileges

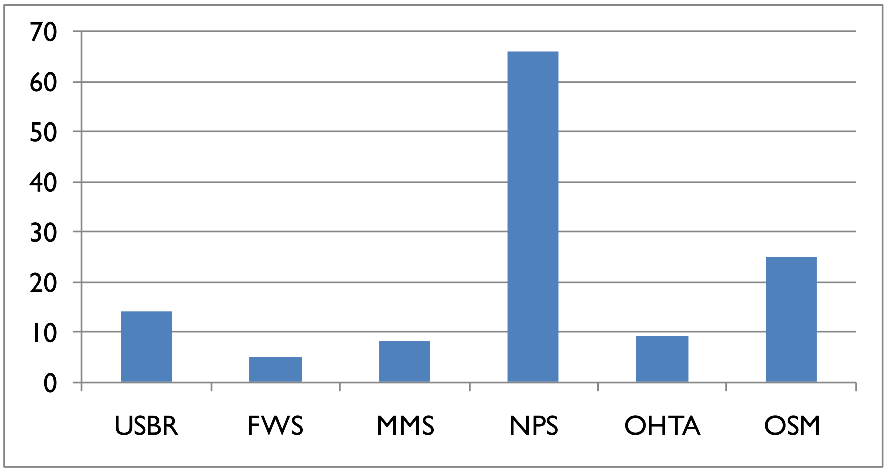


Figure 3. Shows the disparity of percentages of users with elevated privileges, such as “local administrator” or “power user,” among bureaus.

Network Access Control

The Department and bureaus have Plan of Action and Milestones[11] (POAM) with an estimated cost of $3 billion to mitigate the weaknesses associated with network access control. Network access control, required per NIST Special Publication 800-53 (IA-3) and Departmental policy, prevents unauthorized devices from connecting to the network by assuring a device is authenticated.

During fieldwork at three bureaus, we determined that network access control was not deployed to prevent unauthorized computers from connecting to the network. We connected an unauthorized computer to the network and performed scanning that was likely to be detected, and little to none of the activity was identified or reported. We were able to connect to internal Web sites containing sensitive information from the unauthorized computer without being authenticated as a DOI or bureau user.

We also found weak physical security controls.[12] We successfully gained entry and access to offices without any type of identification. Once we were inside bureau facilities, physical access was virtually unrestricted, which enabled logical access to the network. Weak physical security controls coupled with the lack of

[11] POAM ID number 13870.
[12] The Incident Response section contains additional information on weak physical security controls.

network access control implementation could lead to the loss or compromise of sensitive information.

Security Technical Implementation Guides

Security technical implementation guides (STIGs) are security configuration checklists or instructions for configuring an application or product to a particular operational environment (e.g., a computer or network devices). Departmental policy requires that STIGs be used as part of the overall security baseline.

The Department's security configuration policy does not address all operating systems and applications in use across the agency. We determined DOI has additional applications for which they do not have applicable STIGs. In addition, we found users with administrator rights who had installed peer-to-peer applications, games, adult content screensavers, and other unauthorized software that went undetected by the Department despite DOI IT Security policy prohibiting it. The Department cannot create a STIG for unidentified software.

Recommendations

6. Implement least privilege principal and control use of elevated user rights.

7. Standardize Web browsers and firewalls on workstations Interior-wide.

8. Document and approve all deviations from FDCC compliance.

9. Implement network access controls.

Incident Response and Reporting

Policy

FISMA § 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 U.S. Computer Emergency Readiness Team (US-CERT) and notify and consult with law enforcement agencies, including their respective OIG when necessary based on the guidance. Office of Management and Budget's July 12, 2006 memorandum M-06-09[13] also requires that agencies report all incidents involving personally identifiable information (PII) to US-CERT within 1 hour of discovering the incident.

[13] Memorandum M-06-09, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments."

NIST Special Publication 800-61[14] provides guidance for handling IT security incidents. The Interior Computer Security Incident Response Handbook[15] also outlines response and reporting procedures for the agency in sufficient detail, and is consistent with NIST and the DOI IT Security Policy Handbook, which requires bureaus to have an incident response capability.

The Interior Computer Security Incident Response Handbook states that incident response coverage is from 7 a.m. to 7 p.m., Eastern Standard Time. Security Operations personnel act as a point of contact for reporting incidents at the Department and manage the DOI Computer Incident Response Center (CIRC), a centralized database or ticketing system intended to correlate and track incidents at all bureaus.

Procedure Implementation is Lacking

We found that the incident response capability within the Department is fragmented and inconsistent. We identified inconsistencies in how DOI reports incidents to US-CERT. We also identified inconsistencies with bureaus reporting to DOI using the DOI CIRC. We found that bureaus have their own incident-reporting and response policies and procedures, which makes it difficult for the agency to correlate key incidents in a central location. We sampled three bureaus and found that two of them were not aware of the Interior Computer Incident Response Handbook issued in January 2010.

The multiple layers to report an incident to the Department is time intensive and not consistently followed. The lack of a bureau-wide, consolidated approach, coupled with duplicative policy and procedures, is hindering the DOI Incident Response program as a whole.

Absence of Preventative Measures and Breakdown of Procedures

We found that key preventative and incident detection measures were absent and some procedures were disregarded.

Our testing at three bureaus found file and object access not enabled. Having file and object access enabled would allow the bureaus to record and identify OIG or unauthorized personnel's access or attempted access to sensitive information. We found that permissions set to protect sensitive information were generally restrictive throughout the three bureaus but not in all cases. We found that as a domain administrator or local administrator of a server, we were able to view, modify, and copy sensitive information without being detected.
We also found weak physical security controls. At a National Park Service headquarters building, we were able to piggyback into the secure facility with an armed Park Ranger through a door for employees only. Once inside, physical access to the bureau facilities was virtually unrestricted, allowing us to gain logical access to the network and collect hardcopy personally identifiable

[14] Revision 1, "Computer Security Incident Handling Guide," (March 2008).
[15] Version 2, issued on January 28, 2010.

information (PII) and sensitive information. Weak physical security controls led to the loss and compromise of hardcopy sensitive information that was never reported to DOI CIRC. We were 100 percent successful in gaining access to three bureau networks with an unauthorized computer. In some cases, we were able to find and access sensitive information with the unauthorized computer.

Logging in with credentials obtained by successful social engineering attacks could have been prevented if two-factor authentication, the use of two independent authentication methods for authorizing secure access to a system, were implemented. We were 100 percent successful at all three bureaus in obtaining usernames or passwords to log into computers. Two-factor authentication was not enforced on these accounts, as we logged in without a Personal Identity Verification card.

We reviewed incidents within the DOI-CIRC from April 21 through September 14, 2010 and found that only three of 245 PII tickets were reported to US-CERT within the required 1-hour timeframe. Of the 245 PII incidents we reviewed within DOI-CIRC, we found that bureaus took an average of 54 days to report PII incidents to the Department, which delayed the Department's required report to US-CERT. Our testing even created an incident in Alaska. We found that our incident was reported to a trained IT security manager within the state, but the IT security manager never reported it to the bureau level. These stovepipes do not allow the centralized management and correlation of incidents to take place in a timely enough manner so that Departmental procedures can be followed.

Incidents

Our testing of incident response at three bureaus demonstrates the inconsistency with which they identify and report incidents. When we created incidents during our testing, we found reporting in one bureau was timely and accurate but untimely and inaccurate in another. We found the following unreported incidents:

- Unauthorized access to facilities;
- Copy and removal of PII from servers;
- Unauthorized access to documents;
- Removal of hardcopy PII-sensitive documents;
- Social engineering attacks;
- Unauthorized scans of networks;
- Unauthorized computers connected to networks; and
- Passwords cracked on files with weak encryption standards.

We also obtained numerous documents and property from NPS, such as:

- Social Security numbers in hardcopy documents, workstations, and servers;
- Numerous users' personal listings of username and passwords in various formats (e.g., MS Excel, MS Word and text files) for GovTrip,

QuickTime, Interior Department Electronic Acquisition System (IDEAS), and the Federal Financial System;

- Numerous credit card numbers and personal receipts attached;
- Social Security numbers posted to internal Web sites of external vendors or providers;
- Adjudication of security clearances;
- 385 IBM Lotus Notes IDs coupled with a password list, which allow unauthorized access to users' email accounts;
- Sensitive information from unlocked shredder bins; and
- An unlocked workstation with a username and password on the screen.

Of these documents and findings, we found neither that the incidents were reported nor any indication that the bureaus knew these documents had been compromised. Our review demonstrated that incidents were not identified and preventative, and detection measures are not fully in place at the Department.

Recommendations

10. Implement incident response policies and procedures consistently throughout bureaus and offices.

11. Require bureaus and offices to use the Department's DOI-CIRC database for incident response and reporting versus their own implementation.

Security Training

Policy

FISMA has multiple security training requirements designed to inform personnel of information security risks and responsibilities. DOI's annual security training, Federal Information Systems Security Awareness (FISSA), is required by all users. Role-Based Information Technology Security Training is required by those with significant IT responsibilities. All users must annually acknowledge the Rules of Behavior, which detail users' expected behavior with regard to information and information system use.

DOI's FISSA training consolidates Privacy and Records Management and the annual acknowledgement of the Rules of Behavior. According to the DOI IT Security Policy Handbook, FISSA "is required by all information system users before authorizing access to information systems and annually thereafter." Training requirements reiterated in a December 22, 2009 memorandum from the DOI CIO "require all users of Department of the Interior (DOI) information systems to receive annual information security awareness, privacy, and records management training, as well as acknowledging system Rules of Behavior" by July 31, 2010. An April 21, 2010 Office of Management and Budget

Memorandum (M-10-15) details the FY 2010 FISMA reporting requirements and extends the FISSA training requirement to "each employee," not just system users.

The annual requirement for users to complete the Rules of Behavior agreement was established in the CIO's December 22, 2009 memorandum. The DOI IT Security Policy Handbook also states that bureaus shall "ensure receipt of signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information." It further states that bureaus "may leverage electronic signatures for use in acknowledging rules of behavior."

FISMA § 3544(a)3(d) requires role-based IT security training. It specifically requires that the Department's CIO train personnel with significant responsibilities for information security. Also, the DOI IT Security Policy Handbook states that role-based information technology security training "programs are implemented in accordance with the DOI Role-Based IT Security Training Guide, and NIST Special Publication 800-16, 'Information Technology Security Training Requirements: A Role- and Performance-Based Model' (March 20, 2009)." On December 23, 2009, the Department CIO released Office of CIO Directive 2010-002, which detailed role-based information technology security training requirements and released DOI's updated Role-Based Security Training Standard Version 2.5 (November 3, 2009). The directive stated that role-based information technology security training requirements were to be completed no later than July 31, 2010.

Results

FISSA

In general, procedures surrounding FISSA training were well implemented during FY 2010. There were challenges associated with the deployment of a new training system, but the guidance remained consistent and well disseminated throughout DOI. July 31, 2010 reports from the Departmental training system reflect that 97.7 percent of Federal employees and other personnel[16] completed the training. The training course covered DOI security policies and procedures and was determined to be comprehensive.

Despite DOI efforts to provide annual training, users continue to introduce risk to the environment. During unannounced fieldwork at a bureau, we observed a contract employee workstation which was left unlocked, unattended, and logged-in to the bureau email. In addition, the email on the screen contained a user name and password to a bureau File Transfer Protocol (FTP) site. Our review of the FISSA completion records revealed that this contractor had been enrolled and included in the baseline but had not completed the FISSA training.

[16] Other personnel include all types of non-full time equivalents such as contractors, volunteers, and seasonal employees.

Rules of Behavior

Rules of Behavior for each bureau were included as part of FISSA training. Prior to completing the training, users select the rules of behavior appropriate to their specific bureau. The user is asked to read the rules and select “I agree” to progress and finish the course. During FISMA fieldwork, we confirmed that none of the three bureaus retained signed, hard copy versions of the Rules of Behavior acknowledgement. The DOI IT Security Policy Handbook allows electronic signatures to be associated with the Rules of Behavior acknowledgement. The bureaus that we sampled were unsure if the submission in DOI Learn equates to an electronic signature.

Each bureau has its own Rules of Behavior. We determined that most Rules of Behavior documents do not incorporate specific information regarding remote access or teleworking responsibilities.

Role-Based Security Training

Role-Based Security Training is completed by personnel with significant information security responsibilities. The Department’s Role-Based Security Training Standard[17] clearly defines training requirements for each group, bureau responsibilities for tracking completed training, and courses available in DOI Learn. As of July 31, 2010, 54 percent of all personnel required to take role-based security training had completed the required training. The Department extended its reporting date for accepting training completions, and as of September 15, 2010, it reported 96.2 percent completion.

Implementation Challenges

Accurately identifying personnel required to complete FISSA and Role-Based Security training is a challenge for DOI. The Department does not have a central authoritative identity management system for identifying all personnel who have various training requirements. Establishing baselines is a manual process, which provides a point-in-time number based on data from a number of available reports, including the active directory listing, historical training records, payroll, and human resources reports.

Role-based security training completions are tracked in DOI Learn after users “self certify” that they are finished. Supporting artifacts cannot be uploaded into the system as evidence of self certifications. Role-based security training in the Department can only be verified manually, using an extensive data call.

Significant IT Security Duties

Personnel with a range of qualifications and position descriptions perform DOI IT security duties. On December 17, 2009, we issued a data call of all Department personnel with “significant IT security responsibility” to determine the demographics of this group. The list contained employees and non-employees for all bureaus and reflected various portions of their time devoted to IT security

[17] Version 2.5, section 1.5, dated November 3, 2009.

duties. The personnel ranged in General Schedule (GS) grade levels and GS-series. The information was manually compiled by each bureau because an automated method does not exist.

Our analysis evaluated whether IT security is performed by a sufficient number of personnel with an appropriate grade structure and expertise. The results do not reveal a great deal of consistency regarding personnel and those variables impact how IT security is conducted in DOI.

The Department's Role-Based Security Training Standard[18] defines the type of personnel considered as having "significant information security responsibility." In FY 2010, the Department reported 4,067 personnel with "significant IT security responsibility." Our analysis revealed that:

- 536 more personnel were involved in IT security in FY 2010 than FY 2009;
- 77 percent of the personnel were fulltime Federal employees;
- 23 percent of the personnel were contractors;
- The largest gain in personnel was at USGS, which added 142 employees;
- The next largest gain in personnel was at FWS, which added 128 employees;
- The biggest loss in personnel was at USBR, which lost 13 fulltime employees;
- The number of personnel devoting 100 percent of their time to IT security dropped by 36 percent;
- 50 percent of the new 354 fulltime employees are GS-12 or above;
- IT Security personnel increased by 22 percent from FY 2008; and
- 202 fewer people devote at least 60 percent or more of their time to IT security compared to FY 2009.

Figures 4 to 7 show data from our comparative analysis between FYs 2008, 2009, and 2010.

[18] Version 2.5, Section 1.5, dated November 3, 2009.

Personnel Reported (total) Year-by-Year Comparison

	FY 2008		FY 2009			FY 2010		
Bureau	FTE	CNTR	FTE	CNTR	Total Difference	FTE	CNTR	Total Difference
BIA	127	63	148	46	+4	140	63	+9
BLM	601	123	559	94	-71	572	81	0
BOR	328	16	348	62	+66	335	62	-13
FWS	284	63	273	63	-9	403	63	+128
MMS	192	174	210	109	-47	221	174	+76
NBC	292	141	340	232	+139	389	287	+104
NPS	385	10	408	60	+73	440	57	+29
OHA	5	5	6	0	-4	6	0	0
OHTA	5	21	5	21	-	4	18	-4
OS	56	12	63	18	+13	73	45	+37
OSM	37	10	39	8	-	58	10	+21
OST	17	4	21	0	-	27	0	+6
SOL	2	1	6	2	+5	6	3	+1
USGS	327	42	340	48	+19	448	82	+142
Total	**2658**	**685**	**2768**	**763**	**+188**	**3122**	**945**	**+536**
Annual combined total	**3343**		**3531**			**4067**		

Figure 4. Presents the number of fulltime Federal employees and contractor personnel in a year-to-year comparison and how they are allocated to various DOI bureaus.

Employees Reported (by Grade) Year-by-Year Comparison

Grade	FY2008	FY2009	FY2010	Difference (FY08-09)	Difference (FY09-10)
SP-5	1	1	1	-	-
WG-11	2	2	1	-	-1
GS-2	1	1	0	-	-1
GS-3	-	2	4	+2	+2
GS-4	4	7	10	+3	+3
GS-5	24	33	37	+9	+4
GS-6	24	18	24	-6	+6
GS-7	95	94	137	-1	+43
GS-8	15	12	15	-3	+3
GS-9	218	228	278	+10	+50
GS-10	5	4	2	-1	-2
GS-11	513	522	589	+9	+67
GS-12	669	665	743	-4	+78
GS/GM-13	515	562	645	**+47**	**+83**
GS/GM-14	337	366	374	+29	+8
GS/GM-15	154	171	176	+17	+5
SL	5	4	5	-1	+1
SES	74	76	81	+2	+5
Total	2656	2768	3122	**+112**	**+354**

Figure 5. Employees reported by grade, in a year-to-year comparison from FY 2008 to 2010.

Percent of Time Personnel Devoted to IT Security Duties

	FY 2008		**FY 2009**			**FY 2010**		
Percentage	FTE	CNTR	FTE	CNTR	Total difference	FTE	CNTR	Total difference
100	506	83	524	153	+88	380	117	-180
≥ 90	531	91	551	160	+89	406	135	-170
≥ 80	549	97	579	165	+98	432	147	-165
≥ 70	626	103	654	182	+107	463	176	-197
≥ 60	652	116	686	190	+108	492	182	-202
≥ 50	783	134	809	214	+106	625	245	-153
≥ 40	845	151	858	221	+83	682	251	-146
≥ 30	1027	193	1008	247	+35	838	285	-132
≥ 20	1467	329	1510	421	+135	1547	572	+188
≥10	2058	517	2208	599	+232	2419	791	+403
≤ 9	600	168	560	164	-44	704	153	+133

Figure 6. The time personnel devote to IT security has dropped dramatically since 2009.

Employees with Significant Information Security Responsibilities

Job Title	Series	Explanation
Clerk (STEP)	0303	IT Clerk (STEP)
Wild Horse and Burro Specialist	0401	System Manager, Wild Horse and Burro System
Natural Resource Specialist	0401	Active Directory Elevated Privileges
Hydrologist	1315	Security Point of Contact
Geologist	1350	IT Security Administration
Supervisory Geologist	1350	IT Security Manager
Fishery Biologist	0482	Security Point of Contact
Geophysicist	1313	IT Security Administration
Physical Scientist	1301	IT Project Manager
Bankcard Coordinator	0303	System Administrator
Realty Specialist	1170	Active Directory Elevated Privileges
Park Ranger	0025	OU Admin, Information Security Management
Electronic Mechanic	2604	Local Area Network Administrator
Supervisory Budget Officer	0340	Budget Tracking
Pipeline Coordinator Officer	0301	System Owner

Figure 7. A considerable array of personnel who perform information security duties have job titles that do not seem to support the necessary qualifications for IT security functions.

Recommendations

12. Evaluate the current Rules of Behavior submission process to ensure it satisfies electronic signature requirements.

13. Implement a solution that assists in establishing accurate employee and contractor baseline counts, such as a central authoritative identity management system.

14. Review the qualifications of personnel performing IT security duties in the Department and reassign those duties accordingly.

Plan of Action and Milestones

Policy

The Office of Management and Budget has required quarterly system Plans of Action and Milestones (POAM) since October 31, 2001. The Plan of Action and Milestones program has taken steps forward since then but it certainly has not matured into an effective and reliable program for managing all IT weaknesses in the Department.

The DOI IT Security Policy Handbook requires Bureaus and Offices to develop and continuously update Plan of Action and Milestones for all systems. POAMs should document all planned, implemented, and evaluated remedial actions to correct system deficiencies identified during the assessment of the system security controls. The process is to be completed in accordance with the DOI POAM Process Standard. The Department CIO expanded on the policy on September 23, 2008, when he mandated the use of CSAM as the central database for managing POAMs.

Office of Chief Information Officer Directive 2010-006 reiterated this policy on May 18, 2010, and released an updated version on May 10, 2010, “DOI POAM Process Standard” (Version 1.8), incorporating the use of CSAM and automating the process. DOI’s June 2009 “C&A Guide using CSAM Solution v2.0” provides additional details and procedures for maintaining the POAM program using the CSAM solution.

According to NIST Special Publication 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems,” the Plan of Action and Milestones is one of the three key documents in the system authorization package and is used by the authorizing official to monitor progress in correcting weaknesses.

The POAM describes the tasks planned to:

- “Correct any weaknesses or deficiencies in the security controls noted during the assessment;” and
- “Address the residual vulnerabilities in the information system.”

It also identifies:

- “The tasks to be accomplished with a recommendation for completion either before or after information system implementation;
- The resources required to accomplish the tasks;
- Any milestones in meeting the tasks; and
- The scheduled completion dates for the milestones.”

Policy Implementation

All bureaus have complied with Departmental guidance to use the CSAM solution for system Plans of Action and Milestones. Data in the system could be valuable for management and oversight purposes. We determined that the Department, specifically the Cyber Security Division, has initiated oversight efforts to enhance the data quality within CSAM. The Cyber Security Division sent copies of review items to bureaus, instructing them to take corrective action. Based on our analysis, extensive effort is necessary to enhance the Plan of Action and Milestones data quality. In June 2010, a CSAM system failure was followed by an unsuccessful backup. The Department CIO informed users that data was lost back to approximately February 19, 2010. POAM updates entered in the database during that period of time were impacted, but bureaus were not able to fully assess the impact. During our fieldwork they were still in the process of determining what data was lost.

CSAM automates the Plan of Action and Milestones process and enables the OIG to perform efficient analysis of the data. As with any automated system, the output is only as good as the data input. We identified errors, incomplete information, and missing artifacts associated with the Plan of Action and Milestones. A consolidated October 4, 2010 CSAM Plan of Action and Milestones report for all systems showed:

- The total estimated cost associated with Department Plan of Action and Milestones is more than $7 billion ($7,603,531,653);
- Continuous monitoring weaknesses have an estimated $120.5 million associated cost with limited project investment planning;
- Network access control weaknesses have an estimated $3 billion associated cost with limited project investment planning;
- 11,064 Plan of Action and Milestones weaknesses are associated with agency systems;
- 1,141 are associated with contractor systems;
- 3,580 are in delayed status;
- 1,330 have not been started;
- 3,227 did not have an estimated associated cost;
- 5,579 of them estimated the cost to be less than $1,000 each;
- 1,358 Plan of Action and Milestones did not have any milestones;
- 5,808 were completed in an overall average of 277 days (range was 1 to 3,322 days);
- 6,671 did not have an associated artifact posted;
- 16 had blank "detailed weakness descriptions";
- 12 had blank "POAM titles";
- 1,254 had planned finish dates that were blank or to be determined;
- 257 did not include organization priority (i.e., high, medium, or low);
- 487 were identified as mission critical;
- 76 of the 487 mission critical Plan of Action and Milestones were completed on an overall average of 218 days (range was 1 to 868 days);
- 1,634 Plans of Action and Milestones were identified as related to financial systems;
- 853 were missing system status (e.g., development, initiation, operational, or retired); and
- 77 with either incorrect actual start or finish date, as the time to correct was negative.

Using the data above we concluded that bureaus are gathering data in CSAM, but it is not being used to manage IT weaknesses, manage risks, or prioritize corrective action or resource allocation. We further concluded that the data is not being used to perform effective management and oversight of the Plan of Action and Milestones program.

We identified inconsistencies among three bureaus in implementing their Plan of Action and Milestones programs. One of the three bureaus that we reviewed performed further analysis of the data to identify IT controls associated with system Plan of Action and Milestones and various statistics (e.g., delays, milestones, etc.) associated with its Plan of Action and Milestones, but the process was not fully implemented. Bureaus with large, complex systems do not have an established method for combining weaknesses for all component parts of the system. Also, quarterly Plan of Action and Milestones briefings for the authorizing officials are not conducted consistently.

The Impact of CSAM Failure

The Plan of Action and Milestones program was significantly impacted from the CSAM backup failure. During our fieldwork, all three bureaus stated that they experienced data loss and would need additional resources to restore it. Most bureaus were unable to establish a dollar impact but all said it was a big step backward. We were told by one bureau that Plan of Action and Milestones cannot be reentered using historical ID numbers, and therefore tracking capabilities are lost.

Recommendation

15. Ensure that the Department and bureaus are accountable for consistent and accurate data in CSAM to manage Plan of Action and Milestones weaknesses.

Remote Access

Policy

In August 2006, the Chief Information Officer directed all bureaus to transition to the Department's remote access system by January 31, 2007, and a May 2007 Office of Management and Budget memorandum[19] requires two-factor authentication for remote access.

FISMA emphasizes the need for organizations to implement an organization-wide information security program. NIST Special Publication 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," provides details of preparing, operating, and securing remote access solutions.

The DOI IT Security Policy Handbook requires that bureaus mitigate the risk associated with connecting equipment remotely and that access shall be exclusively provided by Government-owned computers. It states the following safeguards must be implemented for remote access:

[19] OMB M-07-16, "Safeguarding against and Responding to the Breach of Personally Identifiable Information."

- Multi-factor authentication;
- Whole disk encryption;
- File and folder encryption;
- Host-based Anti-Virus software;
- Host-based firewall;
- Patch management;
- Security Technical Implementation Guides; and
- Virtual Private Network (VPN) / Encryption of data in transit.

Policy and Telework

The DOI IT Security Policy Handbook provides a set of minimum standard elements for bureaus to address the protection of PII and sensitive data, remote access, and mobile computing device usage in their Rules of Behavior agreement. Copies of bureaus' Rules of Behavior can be accessed in DOI Learn through the training course titled "FY 2010 Annual End-User Federal Information Systems Security Awareness + Privacy and Records Management."

We found a lack of telework or remote access addressed within the Rules of Behavior from bureaus. Also, the Department does not have an up-to-date telework policy addressing security of remote access[20] despite a June 2009 revision to NIST Special Publication 800-46, which states that "a telework security policy should define which forms of remote access the organization permits." We did not find this guidance during our review of the Department's telework policy.

Numerous Solutions for Remote Access

Remote Access is noncompliant with the Office of Management and Budget or DOI mandates. More remote access systems have been added against the Department's direction and two-factor authentication has not been fully implemented. These inconsistencies facilitate an unmanageable remote access environment.

Our analysis of remote access systems uncovered a significant vulnerability at FWS. We found that FWS implemented a remote access solution that the Department did not approve to operate. We immediately notified the Department, and it discontinued the remote access system from connecting through the Department until its risks can be formally assessed. Further analysis revealed that FWS called it a "pilot" and had 100 or more users on the remote access system for about 6 months. The Department's Enterprise Infrastructure Division, which monitors and controls the Department's perimeter, was unaware of FWS's remote access solution.

We also found that BLM, NBC, NPS, and USGS maintain and use separate remote access systems, even 3 years after the January 31, 2007 deadline for

[20] DOI telework policy has not been updated since Personnel Bulletin No. 05-02 first established one on February 18, 2005.

transitioning to the Department's remote access system. FWS was found to have implemented a new remote access solution this year.

Two-Factor Authentication for Remote Access

DOI cannot enforce two-factor authentication for remote solutions because not all personnel have been issued Personal Identity Verification (PIV) cards[21] (for more information, see the Account and Identity management section of this report). The Department does not enforce two-factor authentication with users who have that ability.

We reviewed the Department's connections to the DOI centralized remote access solution in August 2010 and found percentages of users using two-factor authentication varied among bureaus. The Department did not have insight into the disparate remote access for those bureaus.

Department-wide, 22 percent of users logged in, in August 2010, using two-factor authentication for remote access. Bureau compliance ranges from 0 to 100 percent in their use of two-factor authentication. The following percentages show bureau compliance with the use of two-factor remote access within the bureaus:

- OHA: 0 percent;
- FWS: less than 1 percent;
- MMS: 2 percent;
- NBC: 2 percent;
- OS: 3 percent;
- NPS: 6 percent;
- BIA: 12 percent;
- BLM: 35 percent;
- USGS: 47 percent;
- OST: 70 percent;
- OHTA: 77 percent;
- USBR: 94 percent; and
- OSM: 100 percent.

Connections to Remote Access

During our interviews at the bureaus, we found that any computer, such as a personal or public library computer can connect to the Department's remote access solution, despite the DOI IT Security Policy Handbook requirement that only Government computers can access the Department's remote access solution. This means that the Department can only enforce one of the eight safeguards: "Virtual Private Network (VPN) / Encryption of data in transit." The Department has no way to validate that personal computers are configured securely. If the Department enables host checking,[22] DOI can reasonably ensure that only

[21] As of September 30, 2010, 27,326 personnel have yet to be issued PIV cards.

[22] Host checking would allow the Department to authorize remote access connections based on criteria such as security configurations.

authorized Government computers with the proper security configurations can connect to DOI remotely.

Recommendations

16. Consolidate remote access solutions to allow efficiency and reduce duplicative services.

17. Enforce two-factor authentication.

18. Enable host checking for remote access.

19. Update the telework policy from Personnel Bulletin No. 05-02.

Account and Identity Management

Policy

FISMA requires Federal agencies to provide information security for its IT assets. Account and identity management directly correlates with the ability to securely manage IT assets. Homeland Security Presidential Directive 12 mandates the use of standard identification for employees and contractors by October 27, 2009, so as to be compliant with Federal Information Processing Standards[23] and NIST Special Publication 800-63.[24]

DOI Personnel Bulletin 09-06[25] requires compliance with Federal Information Processing Standards 201-1 and Homeland Security Presidential Directive 12. The Chief Information Officer's December 2009 memorandum, "DOI Access Procedures for Bureau/Office Active Directory and Email Systems," recommends that bureaus adhere to new account provisioning procedures and align with DOI Personnel Bulletin 09-06.

The DOI IT Security Policy Handbook requires that bureaus "manage all information system accounts, including establishing, activating, modifying, and reviewing, disabling, and removing accounts…" and "ensure information system accounts are reviewed at least every 3 months."

In a September 27, 2010 management advisory, we expressed concern for simple social engineering techniques that showed a lack of or failure to follow account management procedures. Social engineering results ended in obtaining the username and password for accounts of a Chief Information Security Officer, field office managers, human resources staff, and a domain administrator.

[23] 201-1, "Personal Identity Verification of Federal Employees and Contractors," issued in March 2006.
[24] "Electronic Authentication Guideline," issued in April 2006.
[25] "Policy for the Issuance and Management of DOI Access Cards," issued in June 2009.

The DOI Access Program

Of the three bureaus we reviewed, we found only one bureau following guidance for account provisioning[26] procedures for the DOI Access system as outlined in the Chief Information Officer's December 2009 memorandum.[27] The procedures, however, are ambiguous because they "recommend" instead of specifically direct the intended procedures. This lack of direction caused confusion, and as a result, the Department is neither compliant with nor fully using the DOI Access system.

Also, we found that account management procedures were duplicative and inconsistently implemented and distributed. A major objective behind the procedures is to create new accounts in the DOI Access System. We found that 9 months after the January 15, 2010 deadline, not all accounts were created within the system.

The DOI Access System cannot provide a full identity management program. It contains contractor status only for contractors with DOI network access but not all DOI contractors require DOI network access. The DOI Access system does not manage access to the copious amount of individual DOI applications. Until all contractors and all disparate DOI applications are considered and entered into DOI Access, the Department will continue to lack one authoritative source for identity management.

Personal Identity Verification (PIV) Cards

Implementing the standard identification mandate from Homeland Security Presidential Directive 12 increases IT security because it ensures that people are who they say they are. Standard identification is a significant element to confirming users' identities because it employs a two-factor authentication, which grants a user access only when they can combine something they have with information that they know (e.g., a Personal Identity Verification card and a password or personal identification number).

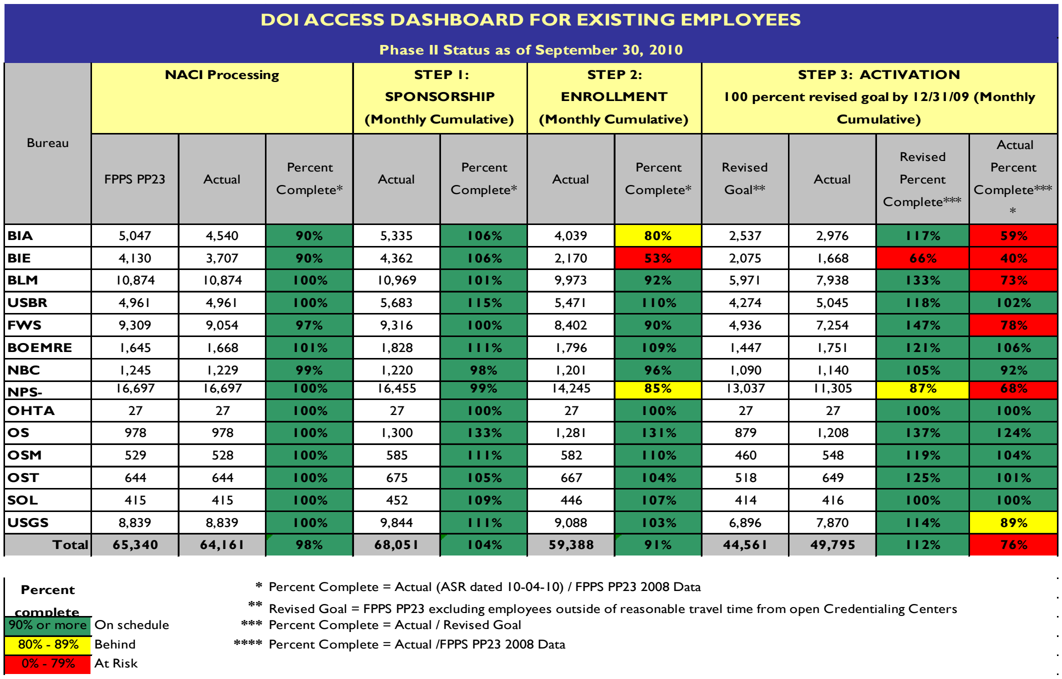
The Department reported a December 31, 2010 completion date to the Office of Management and Budget for integration of PIV credentials with logical and physical access systems. We found, however, that the Department has not yet activated PIV cards to 15,682 employees (24 percent) and 11,637 contractors (78 percent) as of September 30, 2010.

The Department considers the following bureaus at risk. A bureau's risk is attributed to PIV card issuance and in some instances, includes employees, contactors, or both:

- BIA, which is at 59 percent issuance for employees and 2 percent for contractors;

[26] We found OSM at 100 percent compliance, BLM with limited implementation, and NPS testing the procedures at one office.
[27] "DOI Access Procedures for Bureau/Office Active Directory and Email Systems."

- BIE, which is at 40 percent issuance for employees and 2 percent for contractors;
- BLM, which is at 73 percent issuance for employees and 2 percent issuance for contractors;
- NPS, which is at 68 percent issuance for employees and 6 percent for contractors;
- FWS, which is at 78 percent issuance for employees and 9 percent for contractors;
- USBR, which is at 60 percent issuance for contractors;
- BOEMRE, which is at 52 percent issuance for contractors;
- OS, which is at 54 percent issuance for contractors; and
- SOL, which is at 24 percent issuance for contractors.



DOI ACCESS DASHBOARD FOR EXISTING EMPLOYEES

Phase II Status as of September 30, 2010

Bureau	NACI Processing			STEP 1: SPONSORSHIP (Monthly Cumulative)		STEP 2: ENROLLMENT (Monthly Cumulative)		STEP 3: ACTIVATION 100 percent revised goal by 12/31/09 (Monthly Cumulative)			
	FPPS PP23	Actual	Percent Complete*	Actual	Percent Complete*	Actual	Percent Complete*	Revised Goal**	Actual	Revised Percent Complete***	Actual Percent Complete****
BIA	5,047	4,540	90%	5,335	106%	4,039	80%	2,537	2,976	117%	59%
BIE	4,130	3,707	90%	4,362	106%	2,170	53%	2,075	1,668	66%	40%
BLM	10,874	10,874	100%	10,969	101%	9,973	92%	5,971	7,938	133%	73%
USBR	4,961	4,961	100%	5,683	115%	5,471	110%	4,274	5,045	118%	102%
FWS	9,309	9,054	97%	9,316	100%	8,402	90%	4,936	7,254	147%	78%
BOEMRE	1,645	1,668	101%	1,828	111%	1,796	109%	1,447	1,751	121%	106%
NBC	1,245	1,229	99%	1,220	98%	1,201	96%	1,090	1,140	105%	92%
NPS-	16,697	16,697	100%	16,455	99%	14,245	85%	13,037	11,305	87%	68%
OHTA	27	27	100%	27	100%	27	100%	27	27	100%	100%
OS	978	978	100%	1,300	133%	1,281	131%	879	1,208	137%	124%
OSM	529	528	100%	585	111%	582	110%	460	548	119%	104%
OST	644	644	100%	675	105%	667	104%	518	649	125%	101%
SOL	415	415	100%	452	109%	446	107%	414	416	100%	100%
USGS	8,839	8,839	100%	9,844	111%	9,088	103%	6,896	7,870	114%	89%
Total	65,340	64,161	98%	68,051	104%	59,388	91%	44,561	49,795	112%	76%

Percent complete	
🟩 90% or more	On schedule
🟨 80% - 89%	Behind
🟥 0% - 79%	At Risk

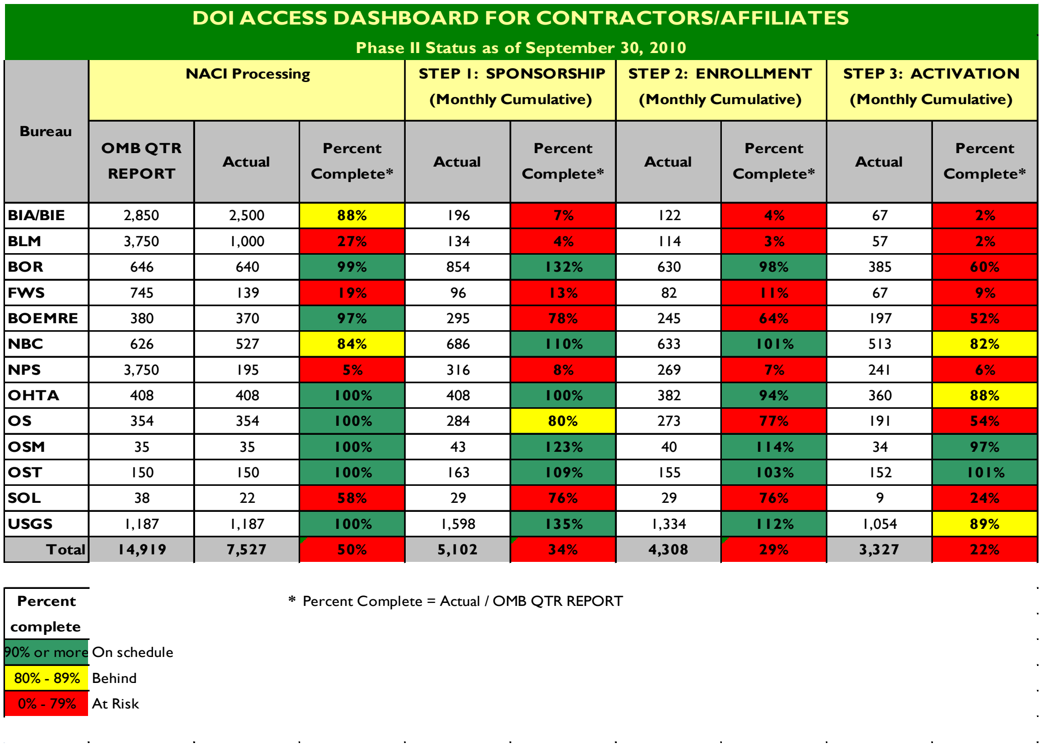
* Percent Complete = Actual (ASR dated 10-04-10) / FPPS PP23 2008 Data

** Revised Goal = FPPS PP23 excluding employees outside of reasonable travel time from open Credentialing Centers

*** Percent Complete = Actual / Revised Goal

**** Percent Complete = Actual /FPPS PP23 2008 Data

Figure 8. Percentages exceeding 100 percent are caused by a fluctuating baseline.



DOI ACCESS DASHBOARD FOR CONTRACTORS/AFFILIATES Phase II Status as of September 30, 2010									
Bureau	NACI Processing			STEP 1: SPONSORSHIP (Monthly Cumulative)		STEP 2: ENROLLMENT (Monthly Cumulative)		STEP 3: ACTIVATION (Monthly Cumulative)	
	OMB QTR REPORT	Actual	Percent Complete*	Actual	Percent Complete*	Actual	Percent Complete*	Actual	Percent Complete*
BIA/BIE	2,850	2,500	88%	196	7%	122	4%	67	2%
BLM	3,750	1,000	27%	134	4%	114	3%	57	2%
BOR	646	640	99%	854	132%	630	98%	385	60%
FWS	745	139	19%	96	13%	82	11%	67	9%
BOEMRE	380	370	97%	295	78%	245	64%	197	52%
NBC	626	527	84%	686	110%	633	101%	513	82%
NPS	3,750	195	5%	316	8%	269	7%	241	6%
OHTA	408	408	100%	408	100%	382	94%	360	88%
OS	354	354	100%	284	80%	273	77%	191	54%
OSM	35	35	100%	43	123%	40	114%	34	97%
OST	150	150	100%	163	109%	155	103%	152	101%
SOL	38	22	58%	29	76%	29	76%	9	24%
USGS	1,187	1,187	100%	1,598	135%	1,334	112%	1,054	89%
Total	14,919	7,527	50%	5,102	34%	4,308	29%	3,327	22%

Percent complete	
90% or more	On schedule
80% - 89%	Behind
0% - 79%	At Risk

* Percent Complete = Actual / OMB QTR REPORT

Figure 9. Percentages exceeding 100 percent are caused by a fluctuating baseline.

The Department has issued PIV cards to 53,122 employees and contractors, but card use is not enforced. This impacts Departmental privacy, data security, authentication, and overall security posture and causes the Department to fall short of compliance with Homeland Security Presidential Directive 12. Full PIV card compliance would mitigate many of the account management issues addressed in the DOI Access Program section.

Other Fieldwork

Active Directory

We conducted an evaluation of Active Directory in February 2010 to assess the efficiency and effectiveness of its information security controls. Active Directory is a Microsoft technology that provides network services that enable applications to use, find, and manage directory resources such as printers, permissions, and users. It unifies management of IT resources such as security, passwords, users and groups.

We found no standardization for naming conventions, how group policies are structured, creating accounts, or monitoring accounts. In some cases, we even found that a lack of standardization for account management existed within the same bureau.

Capabilities to secure user accounts exist in Active Directory. These capabilities include locking accounts to specific workstations, locking them only to certain hours during the day, or setting them to disable after a certain date. We found that those capabilities were either not consistently implemented or not used at all. We also found training account usernames and passwords on sticky notes posted to workstations, which allows anyone with access to these workstations to log into the account from anywhere in the bureau.

FISMA Fieldwork

We identified inconsistent and poor account management practices during our FISMA review of three bureaus. We found that:

- One NPS helpdesk did not follow procedures for changing passwords;
- Four BLM State helpdesks did not follow procedures for changing passwords, which resulted in four successful social engineering exploits;
- Answers to the BLM National Helpdesk's challenge questions were found on the Internet. These weak questions led to a successful social engineering exploit; and
- The OSM helpdesk did not have adequate procedures to validate users calling in for password changes. We obtained a password for the Chief Information Security Officer.

Recommendations

20. Ensure account management procedures adhere to policies.

21. Ensure identity verification security questions are unique and answers cannot be easily obtained.

22. Issue PIV cards to all employees and contractors.

23. Enforce the use of PIV cards for all employees and contractors.

Continuous Monitoring

Policy

A continuous monitoring program encompasses all automated and manual processes implemented in the environment to maintain awareness regarding the organization's security posture. According to NIST, "the objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur." Neither DOI nor its bureaus have an established continuous monitoring strategy even though it is required by FISMA.

Continuous monitoring is integral to NIST Special Publication 800-37,[28] Revision 1, and NIST expects the updated guidance to be fully implemented by February 2011. The Office of Management and Budget elaborates in M-10-15,[29] stating that 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 3-year authorization cycle."

Continuous monitoring policies are disparate or lacking at many of the Department's bureaus and offices. We found draft policy at five bureaus, undeveloped policy at three bureaus, and no policy at five bureaus. Without well-defined policies and coordinated procedures for continuous monitoring, the program is fragmented.

Fragmented Continuous Monitoring

The Department and bureaus have Plan of Action and Milestones[30] (POAM) with an estimated cost of $120.5 million to mitigate the weaknesses associated with continuous monitoring.

According to NIST, continuous monitoring programs include: configuration management, security impact analyses on proposed or actual changes, assessments of selected security controls, and active involvement by authorizing officials in the ongoing management of information system security risks. Accomplishing the objectives of the program would require an effective mechanism to update security plans, security assessment reports, and POAM. Also, assessing the ongoing security posture will demand vulnerability scanning tools, network monitoring tools, and other automated support tools that can help determine the security state of an information system.

The Department's Enterprise Infrastructure Division has a multitude of automated capabilities for continuous monitoring, but full implementation has not occurred. Enterprise Services Network, a part of the Enterprise Infrastructure Division, has the technical capabilities to provide continuous monitoring services as detailed in its "Service Catalogue." Bureaus lack consistency as to which services to leverage. We found that DOI fails to integrate data feeds that would facilitate the maturation of the continuous monitoring program. The feeds would encourage a more timely and efficient data collection process.

We found that the Department's Data Loss Prevention system can identify and report personally identifiable information (PII) incidents but cannot prevent them. The system's next phase of implementation is to prevent PII incidents but resource limitations hinder progress. The Enterprise Services Network at the

[28] Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010.

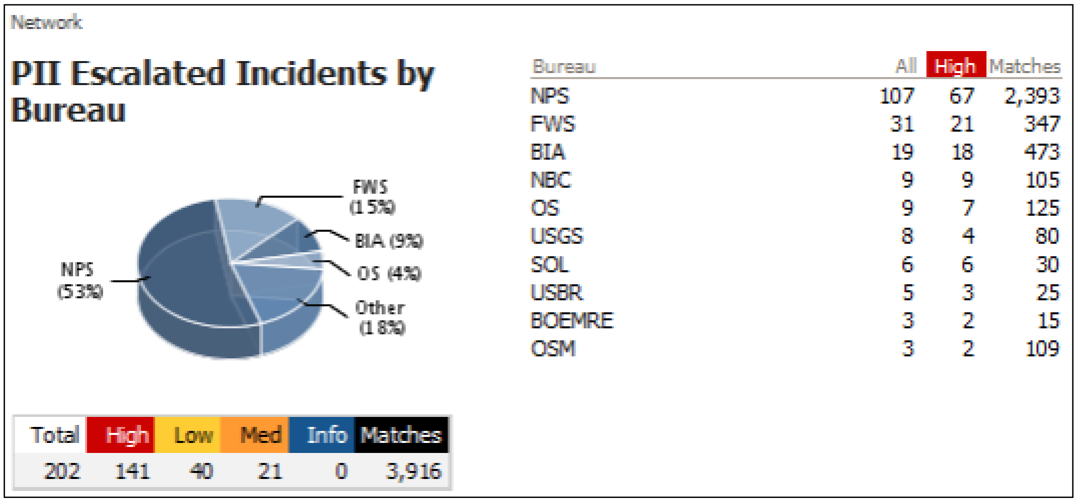
[29] "FY2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."

[30] Continuous Monitoring POAMs: Department CSAM ID numbers 10918 and 13963; 102 Bureau POAMs associated with 74 systems.

Department's Security Operations Center assesses and manages PII incidents, but it does not have sufficient resources to manage them all. Bureaus assist Departmental personnel by managing their own PII incidents.

We found that only BLM and USGS personnel who manage their bureau's PII incidents are at the Security Operations Center on a fulltime basis. BIA, NPS, OSM, and MMS are managing their incidents at the Security Operations Center on a part-time basis. The remaining bureaus do not assist Security Operations Center personnel with managing PII incidents. More than 200 PII incidents are waiting for remedy within the Department's Data Loss Prevention solution as of September 30, 2010.

PII Escalated Incidents by Bureau



Network

PII Escalated Incidents by Bureau

Bureau	All	High	Matches
NPS	107	67	2,393
FWS	31	21	347
BIA	19	18	473
NBC	9	9	105
OS	9	7	125
USGS	8	4	80
SOL	6	6	30
USBR	5	3	25
BOEMRE	3	2	15
OSM	3	2	109

Total	High	Low	Med	Info	Matches
202	141	40	21	0	3,916

Figure 10. This is a snapshot of the Department's Data Loss Prevention system from June 1 to September 30, 2010. More than 200 PII incidents are waiting to be remedied.

Our fieldwork at three bureaus also revealed ad hoc continuous monitoring programs. The bureaus would conduct vulnerability scanning, application patching, and vulnerability mitigation as time permitted or urgency demanded. We found that endpoint protection applications were not properly configured to report to a central location so that bureaus could assess the identified situation on time.

We also determined that monitoring software for Active Directory was not configured to monitor significant events associated with user accounts. Risks cannot be assessed and managed if automated systems are not continually monitoring, if data is not analyzed, if trends are not established, and if reports to management personnel are not occurring.

Security Status Reports

To assess risks, authorizing officials need ongoing results from continuous monitoring, updated security plans, security assessment reports, and POAMs. We found only one example of a complete security status report, prepared for Enterprise Services Network, a system in our sample. The reporting, however, did not occur regularly. DOI guidance suggests neither the format nor content for a security status report.

Unused Investments

We found that many continuous monitoring investments are sitting idle or largely unused. A Departmental system called OPNET is capable of mapping the DOI network and identifying IT assets. It can help detect changes in the network infrastructure and provide an accurate and dynamic IT asset inventory for successful continuous monitoring, but these processes have not been completed because bureaus have not agreed to network adjustments that would enable the process.

Not all bureaus have the system configured to report to an application for Active Directory security enhancements, which would assist with monitoring user account management. We also found an asset inventory, auditing, and logging system that can pull hardware and software reports and provide patch management status. This DOI system sits idle because the bureaus have not made the necessary changes to report to the Department.

Recommendations

24. Create a comprehensive, enterprise-wide strategy for continuous monitoring.

25. Establish a format and content template for the authorizing official's security status reports.

26. Enhance the Department's continuous monitoring program using existing investments.

27. Ensure that bureaus are reporting to centralized Departmental continuous monitoring systems.

28. Establish procedures for using a security assessment report and design a format and content template.

Contingency Planning

Policy

FISMA requires that information system contingency plans be part of DOI's IT security program. The DOI IT Security Policy Handbook clearly states that bureaus "develop and implement contingency plans for all information systems." DOI policy also requires annual plan testing and personnel training regarding their roles and responsibilities in executing the plan.

Plans should be documented in accordance with NIST Special Publication 800-34[31], which addresses contingency planning more extensively than any of the available DOI guidance. According to NIST, guidance must be fully implemented by May 2011.

DOI guidance does not provide DOI system users with adequate information to establish a suite of plans related to the contingency or enough information to understand how their system plan fits into a larger, emergency-preparedness program.[32] DOI guidance needs to be improved significantly to assure system contingency plans comply with NIST.

Contingency plans and testing

We found that contingency plans generally are poorly documented, not based on realistic consideration of threats, and have not been annually updated and tested. The plans in our sample described the planning process, rather than realistic threats and proposed measures to reduce their impact.

Information system contingency plan tests are intended to evaluate the viability of a plan, and identify deficiencies and lessons learned. Although FISMA requires annual, documented tests, we found that many testing scenarios were simplistic and provided limited documentation and conclusions to justify the worth of plan testing.

The backup failure associated with the Office of the Chief Information Officer's own CSAM solution was a major setback that exemplifies the importance of contingency plan testing. System backup and recovery procedures are part of contingency planning; they are to be tested annually in accordance with DOI policy. In the case of the CSAM failure, not all bureaus retained duplicate documentation that could be used for restoration. Had CSAM's contingency plan been tested, it is likely the backup "glitch" would have been detected earlier and potentially mitigated its impact.

We found many areas where plans in our sample fell short. Eight plans have not been updated within the last year, as required. One contingency plan had not been

[31] Revision 1 of NIST Special Publication 800-34, titled "Contingency Planning Guide for Federal Systems," was released in May 2010.

[32] "Certification and Accreditation (C&A) Guide Using the Cyber Security Assessment and Management (CSAM) Solution Version 2.0."

updated since 2006. We also identified eight systems that did not conduct timely contingency plan tests and three that failed to provide any artifacts to document the test.

We also found that contingency plans for systems with high security categorization also were not tested or updated on time. Specifically, we noted that six of the 10 DOI systems were not tested annually, and seven of the 10 plans were not updated annually as is required for all information system contingency plans.

Large, complex systems have not established a contingency plan or even a strategy to consolidate a plan for General Support Systems. Bureaus with large, complex systems have not documented their process for combining the component plans into a consolidated plan for the entire system. We determined some of the component plans have not been updated since 2004. Outdated contingency plans for the component parts are not useful when considering contingency planning for the whole system.

We found that bureaus' various interpretations of the contingency planning process have resulted in inconsistent implementation. According to NIST Special Publication 800-34, "universally accepted definitions for information system contingency planning and the related planning areas have not been available. Occasionally, this leads to confusion regarding the actual scope and purpose of various types of plans." DOI guidance does not address key contingency planning areas, including business impact analysis, business continuity plans, and disaster recovery plans.

Lack of Integration

During our fieldwork, we asked how the bureaus incorporate their information system contingency plans into their overall risk-management, security, and emergency-preparedness programs. We found that the system contingency plans were not considered as part of the bureaus' or location's emergency-preparedness programs. We found one system contingency plan in our sample had been incorporated into a combined contingency plan for all IT operations at that location. The individual information system contingency plans had been considered in aggregate to establish a larger, integrated plan. DOI is unfamiliar with the concept that a suite of plans would be necessary in the event of a disruption. The response, continuity, recovery, and resumption of mission and business functions and information systems are situational, but bureaus have no comprehensive planning guidance to follow.

Recommendation

29. Update contingency planning guidance to correspond with NIST Special Publication 800-34, Revision 1, before May 2011.

Oversight of Contractor Systems

Policy

Overall, Departmental policy regarding contractor oversight is lacking, even though FISMA's requirements for information security also apply to contractor systems,[33] and responsibility and accountability reside with DOI.

FISMA requirements and contractor oversight are addressed in multiple sources of Federal guidance. Interdependencies exist between the various sources of guidance, and coordinated oversight practices are required to ensure effectiveness. Federal Acquisition Regulations (FAR) emphasize the IT security requirements that are included in acquisition documents. The security requirements are much more extensive than just the clauses included in the acquisition documents. FISMA requires that contractors comply with the contracting agency's IT security policies for their program. NIST and OMB provide guidance for implementing FISMA, which often includes requirements for contractors. All four sources (FAR, agency policies, NIST, and OMB) require oversight of contractors. Focusing on any one of the four sources of guidance narrows contractor oversight requirements and does not address the comprehensiveness of the IT security requirements.

The DOI IT Security Policy Handbook does not address contractor oversight responsibilities beyond the capital planning process. It only includes language to be included with Exhibit 300, the business case submission to the OMB for IT capital projects. Also, Departmental policy neither addresses ongoing oversight responsibilities and how the efforts should be documented nor does it provide clear guidance for identifying contractor systems in inventory (for more information, see the IT Inventory section of this report).

Policy Weaknesses

An April 2005 U.S. Government Accountability Office report identified oversight weaknesses of contractors who provide IT systems and services.[34] Also, independent auditors conducting the FY 2010 DOI Financial System Audit identified contractor monitoring concerns in a Notice of Finding and Recommendation (NFR DOI-2010-0007). Specifically, they found that "DOI does not have a centralized system to accurately track the entire population of contractors with access to Interior's IT systems."

[33] FISMA § 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 that each agency provide information security for the 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."

[34] Report No. GAO-05-362, titled "Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors can Reduce Risk."

Impact

Full identification of contractors and contractor systems is fundamental to contractor oversight responsibilities. DOI Access is issuing PIV cards to 14,947 contractors and, to date, has issued them to only 23 percent of the contractors (see the Identity and Account Management section of this report). The DOI IT system inventory identifies 23 accredited contractor systems. During our review of the sample of systems, however, we found three components with contractor-provided IT services or equipment not clearly identified in DOI IT inventory. Assuring the implementation of oversight procedures is impossible if components are not clearly identified in inventory, just as it is impossible to assure contractor compliance with various FISMA requirements if DOI cannot accurately identify them.

Vague guidance statements regarding applicability to contractors are found throughout Department policies. The procedures for contractor oversight are not detailed nor are the documentation requirements defined. We found no clear evidence that the contractor oversight processes have been implemented, but we did see references to contractor operations comingled with agency assessments. Roles and responsibilities for the IT security program elements are not clearly delineated between DOI and contractors.

Bureaus that are required to perform contractor oversight have not established or followed a systematic process, and DOI does not have specific policies for overseeing contractor security practices. The ramifications of not performing contractor oversight significantly impacts identification risk and compliance with FISMA, NIST, Office of Management and Budget, and FAR.

The Department cannot have assurance of its security posture for multiple IT security program areas without contractor oversight of the following:

- Annual assessment of controls at contractor locations;
- Completed IT inventory;
- Security training (role-based security and FISSA training);
- Personnel security (background investigations);
- Physical security (security of data, facility, systems);
- Privileged access to Federal data and systems;
- Oversight of sub-contractors at a contract facility;
- Information controls (privacy) over shared environments;
- Interconnection security agreements and memorandum of understanding;
- The DOI Access process for contractors;
- FDCC compliance;
- Encryption when transporting data;
- Ongoing risk assessments;
- Completions of e-risk authentications; and
- Contractors' system maintenance (e.g., patching, virus protection, scanning, etc.).

Contracting Practices — Hardware and Software Purchases

IT acquisitions are not centrally managed within DOI or bureaus. During fieldwork, we determined that hardware and software purchase generally occur in three ways: under the DOI blanket purchase agreements, General Services Administration schedule (IT Schedule 70), or direct purchase at various bureau levels. We were unable to validate that FAR, parts 39 and 39 D[35], were consistently included on contracts managed at the bureau level. During fieldwork, we were told that personnel with direct purchase authority routinely purchase hardware. Such purchases make maintaining an accurate IT Inventory difficult and DOI is not assured they are obtaining secure configurations. We found that copies of contracts for workstation acquisitions did not include FDCC requirements.

We determined that IT security requirements were not consistently included in IT service contracts. We found some security requirements added to some service contracts, but the content varied significantly between bureaus. Furthermore, we determined that the oversight requirements were not specifically referenced or stated.

We also found that bureaus purchase software outside of the Department's enterprise license agreements or blanket purchase agreements, so discounted rates are not applied. From 1999 to 2009, bureaus purchased 7 percent of their Adobe products outside of Department contracts. Symantec, an end-point security provider in DOI, stated that "the current enterprise agreement is only about 50 percent" of what the bureaus spend with Symantec annually. Such purchases increase the overall costs associated with software purchases. Without the ability to control software acquisitions, the Department cannot ensure efficient spending and standardized software.

Recommendations

30. Define, document, and establish procedures for contactor oversight in accordance with FISMA requirements.

31. Coordinate between IT security and the associated procurement contracting office.

[35] Part 39 of the Federal Acquisition Regulation (FAR) requires agencies to include appropriate information technology security policies and requirements when acquiring information technology, and Part 39d incorporates requirements for using common security configurations.

Conclusion and Recommendations

Conclusion

Poor information in management information systems and inconsistent implementation continues to impact the DOI IT security program. Bureaus will remain unaccountable for their IT security shortcomings and inconsistencies will persist until they are required to follow DOI policy and guidance. Fundamental program components must improve or they will continue to struggle to satisfy FISMA requirements.

Recommendation Summary

To address the deficiencies identified in this report, we recommend that DOI:

1. Standardize the use of terms within CSAM.

2. Establish clear guidance for managing IT assets system inventory, including: the identification and documentation of minor applications, the identification (description, hosted, or operated) and documentation of contractor components, a process for adding systems in development to inventory, a process for adding test systems into inventory, and a process for mapping all components to authorization boundaries.

3. Establish clear guidance for managing hardware and software asset inventory.

4. Update DOI's security authorization policy and guidance to incorporate the latest NIST guidance (NIST 800-37, Revision 1, and NIST 800-53, Revision 3).

5. Merge the multiple DOI security authorization procedural documents into a single document. The guidance should clarify when the authorization process begins in the life cycle, the role of the senior risk executive, and clarify how information system boundaries are to be documented.

6. Implement least privilege principal and control use of elevated user rights.

7. Standardize Web browsers and firewalls on workstations Interior-wide.

8. Document and approve all deviations from FDCC compliance.

9. Implement network access controls.

10. Implement incident response policies and procedures consistently throughout bureaus and offices.

11. Require bureaus and offices to use the Department’s DOI CIRC database for incident response and reporting versus their own implementation.

12. Evaluate the current Rules of Behavior submission process to ensure it satisfies electronic signature requirements.

13. Implement a solution that assists in establishing accurate employee and contractor baseline counts, such as a central authoritative identity management system.

14. Review the qualifications of personnel performing IT security duties in the Department and reassign those duties accordingly.

15. Ensure that the Department and bureaus are accountable for accurate data in CSAM to manage Plan of Action and Milestones weaknesses.

16. Consolidate remote access solutions to allow efficiency and reduce duplicative services.

17. Enforce two-factor authentication.

18. Enable host checking for remote access.

19. Update the telework policy from Personnel Bulletin No. 05-02.

20. Ensure account management procedures adhere to policies.

21. Ensure identity verification security questions are unique and answers cannot be easily obtained.

22. Issue PIV cards to all employees and contractors.

23. Enforce the use of PIV cards for all employees and contractors.

24. Create a comprehensive, enterprise-wide strategy for continuous monitoring.

25. Establish a format and content template for the authorizing official’s security status reports.

26. Enhance the Department’s continuous monitoring program using existing investments.

27. Ensure that bureaus are reporting to centralized Departmental continuous monitoring systems.

28. Establish procedures for using a security assessment report and design a format and content template.

29. Update contingency planning guidance to correspond with NIST Special Publication 800-34, Revision 1, before May 2011.

30. Define, document, and establish procedures for contactor oversight in accordance with FISMA requirements.

31. Coordinate between IT security and the associated contract procurement office.

Appendix 1: Scope and Methodology

Scope

We conducted technical configuration testing at all bureaus, except the Office of Hearings and Appeals, and comprehensive IT security program fieldwork to include interviews, observations, and source documents at three bureaus:

- The National Park Service
  - National Information Technology Center (NITC) and Washington Support Office, Washington, DC, August 30 to September 2, 2010;
  - National Information Service Center, Lakewood, CO, September 15, 2010; and
  - Rocky Mountain National Park, Estes Park, CO, September 20 and 21, 2010.
- The Office of Surface and Mining
  - Office of the Chief Information Officer, Washington, DC, August 4 to August 6, 2010.
- The Bureau of Land Management
  - Information Resource Management, IT Security Division (WO-590), Washington, DC, July 26 to July 28, 2010.

We selected a sample of 21 systems, which represent accreditation boundaries, components of a larger boundary, or systems identified in the DOI environment.

FISMA Sample of Systems for Fiscal Year 2010

Sample No.	System Name	Acronym	Security Categorization
1	Native American Student Information System	NASIS	moderate
2	Land Records Information System	LRIS	moderate
3	BLM GSS	BLM GSS	moderate
4	LAWNET	LAWNET	moderate
5	NIFCeNET GSS	NIFCeNET	moderate
6	National Conservation Training Center Local Area Network NCTC LAN	NCTC	moderate
7	Talent Management System	TMS	moderate
8	AMAG Physical Acess Control System	AMAG	moderate
9	NPS-GSS (Yosemite Wilderness Permit System)	OneGSS (Permit)	moderate
10	NPS-GSS (Concessions Management System)	OneGSS (Concession)	moderate
11	Technical Information Management System	TIMS	moderate
12	OHTA Clifton Gunderson Indian Trust Information System	OHTA-CGITIS	high
13	DOI Enterprise Services Network	ESN	moderate
14	Incident Management Analysis and Reporting System	IMARS	not categorized
15	Project Portfolio System	PPM	not categorized

16	Radio Systems (BLM, NPS, USGS)	Radio	not categorized
17	OSM Enterprise GSS	OSM-GSS	moderate
18	OST LAN/WAN	OSTNet	moderate
19	SOL-NET	SOL-NET	moderate
20	Science and Support System - Moderate	S&SS-Moderate	moderate
21	Science and Support System - Low	S&SS - Low	low

Within this sample, we looked beyond authorization packages to assess DOI's process for managing all IT system inventory. The authorization packages in our sample included most bureaus, all security categorizations (i.e., high, moderate, and low), and all types of systems (e.g., general support systems, major application, minor applications, and undetermined), operational status (i.e., development and operational), and agency and contractor systems.

We based our analysis on data calls issued to the Department and bureaus during fiscal year 2010. We completed additional analysis using information obtained from two Departmental systems: DOI Enterprise Architecture Repository (DEAR) and Cyber Security Assessment Management (CSAM) solution. We reviewed applicable laws, regulations, Office of Management and Budget guidance, National Institute of Standards and Technology standards, Government Accountability Office reports, and Department and bureau policies. All applicable standards and guidance were used as baselines for assessing the DOI IT security program.

Methodology

FISMA requires agencies to have an annual independent evaluation of their information security program and practices and for agencies to report results of the evaluation to the Office of Management and Budget.

We conducted our FY 2010 FISMA evaluation to obtain information required for Office of Management and Budget reporting. This report consolidates our findings related to the Department of the Interior's IT Security Program and their compliance with key FISMA areas.

We conducted our evaluation in accordance with the "Quality Standards for Inspections" as put forth by the Council of Inspector General on Integrity and Efficiency. Accordingly, we included such tests and other procedures that we considered necessary under the circumstances. The conclusions in this report are based on our fieldwork, technical testing, data calls, and analysis of data in Departmental systems.

Appendix 2: Summary of FISMA Results (FY 2003 to 2010)

DOI spent an estimated $719.6 million on IT security since fiscal year (FY) 2003, but FISMA noncompliance persists. Continued funding to DOI's IT Security Program as it is structured is inconsistent with OMB's intent according to a December 21, 2004 advisory (A-123, "Management's Responsibility for Internal Control"), 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 following is a summary of conclusions from DOI FISMA evaluation reports and the associated IT funding by fiscal year, beginning with 2003.

FY 2003

IT Budget: $791.2[36] million, or 5.7 percent of the DOI's overall budget ($13,881 million).[37]
FISMA report conclusion: "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."

FY 2004

IT Budget: $816.5 million, or 5.7 percent of the DOI's overall budget ($14,325 million).
FISMA report conclusion: "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."

FY 2005

IT Budget: $802.8 million, or 5.7 percent of the DOI's overall budget ($15,839 million).
FISMA report conclusion: "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

[36] IT Budget was estimated for FY 2003, FY 2004 and FY 2005 using the average of the FY 2006-2009 IT percentages.
[37] The total DOI Budget for each fiscal year can be found at http://www.doi.gov/budget.

are not implementing DOI policies and are not complying with OMB requirements for Certification and Accreditation."

FY 2006

IT Budget: $934.0 million,[38] or roughly 5.8 percent of DOI's overall budget ($16,122 million).

FISMA report conclusion: "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."

FY 2007

IT Budget: $957.6 million, or roughly 6.1 percent of DOI's overall budget ($15,799 million).

FISMA report conclusion: "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."

FY 2008

IT Budget: $952.7 million, or roughly 5.4 percent of DOI's overall budget ($17,475 million).

FISMA report conclusion: "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."

FY 2009

IT Budget: $965 million, or roughly 5.6 percent of DOI's overall budget ($17,183 million).

FISMA report conclusion: "As in previous years, we found DOI does not fully comply with the FISMA. The decentralized organizational

[38] IT Investment Portfolio amounts are from Exhibit 53 for each fiscal year.

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."

FY 2010

IT Budget: $995.7 million or 8.2 percent of the DOI overall budget ($12,587 million).
FISMA report conclusion: Poor information in management information systems and inconsistent implementation continues to impact the DOI IT security program. Bureaus will remain unaccountable for their IT security shortcomings and inconsistencies will persist until they are required to follow DOI policy and guidance. Fundamental program components must improve or they will continue to struggle to satisfy FISMA requirements.

FY 2011

IT Budget: $981.8 million (proposed) or 8.05 percent of the DOI overall budget ($12,200 million).

Appendix 3: Related OIG Reports, Management Advisories, and Evaluations

A list of summaries and updates, if applicable, for OIG reports and management advisories related to IT's Information Security Program and the fiscal year (FY) 2010 FISMA Evaluation is included below.

FY 2010

Management Advisory: "Account Management," September 27, 2010, documented occurrences of successful social engineering. It identified a lack of user account management procedures resulting in user accounts being compromised and gaining unauthorized network access.

Report: "Evaluation of the Active Directory," No. ISD-EV-MOA-0006-2010, August 2010, documented a lack of standardization in the Active Directory structure, unused investments, and a lack of separation of duties.

Report: "Privacy Impact Assessment," No. ISD-EV-MOA-0005-2010, June 2010, documented inconsistencies in implementing Privacy Impact Assessment requirements. We found processes for Privacy Impact Assessment requirements and Privacy Impact Assessments for IT systems have not been completed to identify privacy risks associated with sensitive information.

Report: "Information Security Evaluation of the National Interagency Fire Center," No. ISD-EV-MOA-0003-2010, June 2010, documented the lack of standardization, duplication, and redundancies at DOI bureaus that are co-located. In addition, radio systems were not certified and accredited.

Management Advisory: "Deficiencies in System Inventory Technology," OIG Case No. PI-PI-10-0045-1, March 2, 2010, documented the lack of accountability for hard drives of former DOI political appointees.

FY 2009

Management Advisory: "Waste and Noncompliance in Departmental Information Systems," October 15, 2009, documented that a vulnerability scanning system is underused and managed inconsistently with FISMA requirements.
Update: No change identified during FY 2010.

Evaluation: "Computer Configuration Evaluation," No. ISD-EV-MOA-0003-2009, August 2009, documented broad noncompliance with

mandatory Federal standards associated with the Federal Desktop Core Configuration as well as OMB and Departmental policy.
Update: We conducted similar testing in FY 2010 and the results are included in this FISMA report.

Management Advisory: “Waste in implementation of Data Encryption Solution,” April 8, 2009, documented $57,000 per month wasted by failing to implement a purchased encryption solution and the additional incurring maintenance costs.
Update: The encryption solution has not yet been fully implemented as of FY 2010.

FY 2008

Report: “Compilation of Information Technology Challenges at the DOI,” May 2008, documented the need to rescind Secretarial Order 3244.
Update: No action has been taken.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in government concern everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement 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