U.S. DEPARTMENT OF THE INTERIOR

OFFICE OF INSPECTOR GENERAL

Verification of Previous Office of Inspector General Recommendations

September 2009

ISD-EV-MOA-0002-2009

Contents

Acronyms and Other Reference Terms

BLM	Bureau of Land Management
BOR	Bureau of Reclamation
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment Management
CSD	Cyber Security Division
Department	Department of the Interior
DOI	Department of the Interior
ESN	Enterprise Services Network
FFMIA	Federal Financial Management Improvement Act
FISMA	Federal Information Security Management Act
FWS	U.S. Fish and Wildlife Service
ISD	Information Security Division
IT	Information Technology
MMS	Minerals Management Service
NBC	National Business Center
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Office of the Secretary
POAM	Plan of Action and Milestones
SP	Special Publication
USGS	United States Geological Survey
WCVF	Weakness Completion Verification Form

Results In Brief

We conducted this evaluation between February 1, 2009, and July 31, 2009. We found 46 recommendations reported closed, 27 recommendations fully resolved, and 19 recommendations not fully satisfied.

The results showed that management oversight of resolving OIG information security recommendations was inadequate, and that a recent investment in a tracking system, Cyber Security Assessment Management (CSAM), to improve information security was not fully leveraged. The Department was not reviewing and monitoring information available within CSAM. Documents and supporting artifacts, such as screenshots, uploaded to CSAM did not always support closure or resolution of the recommendation. Many artifacts were not pertinent to the issue, some were incomplete, and others were too vague. Other artifacts did not provide substantive evidence that the corrective action was completed.

We found no evidence the Department had conducted inspections or tests to determine if our information security recommendations were actually resolved as reported. In several cases, documents and supporting artifacts we deemed insufficient during our FY 2008 evaluations either remained in CSAM or resubmitted without supplemental support for subsequent closure. In some cases, unresolved recommendations remained in a "closed" status for several months until we brought discrepancies to the Department's attention. Furthermore, CSD has no trained information security evaluators or inspectors on staff and lacks the necessary work force and expertise required to perform adequate management oversight.

Weak or missing management poses an ongoing threat to Departmental missions and constitutes a significant deficiency under the Federal Information Security Management Act (FISMA). According to FISMA §3544(c)3(A), a significant deficiency under FISMA must be reported as a "material weakness" under the Federal Financial Management Improvement Act. The electronic data necessary to conduct the Department's various missions safely, effectively, and efficiently are stored and processed by information systems that are at potential risk of compromise or failure, which ultimately could affect the data's integrity. Electronic data stored or processed on these systems may be irreplaceable. If unauthorized persons access this data undetected, bureaus and offices could make improper decisions regarding the environment, wildlife, or national security.

Background

In Fiscal Year (FY) 2007, the Office of Inspector General (OIG) made 125 recommendations to improve information security to the Office of the Secretary (OS) and five bureaus: the Bureau of Reclamation (BOR), Bureau of Land Management (BLM), Minerals Management Service

(MMS), National Business Center (NBC), and United States Geological Survey (USGS). In FY 2008, we conducted six evaluations to assess progress in resolving recommendations. Our evaluations determined that many bureaus made little progress in implementing corrective actions, and many updates they provided were incomplete or inaccurate. In addition, the Department lost an FY 2007 report detailing serious technical vulnerabilities in one of the President's e-government systems. The OIG recommendations made in FY 2007 include compliance with legislation and policy, as well as the enhancement of information security at the Department.

The Department Manual requires the Department's Information Technology Security Staff, such as the Cyber Security Division (CSD), to perform oversight. In addition, the Department Manual requires the Department's Chief Information Security Officer (CISO) to oversee "bureau compliance with Federal and Departmental policies, guidelines, and regulations governing IT security." In response to our FY 2008 evaluations, the CSD established a new process to track and monitor unresolved OIG information security recommendations.

We conducted this evaluation to assess bureau progress in implementing corrective actions for the FY 2007 information security recommendations, as well as to evaluate the effectiveness of the Department's oversight of corrective actions.

Process for Tracking Recommendations

Since July 2008, the use of CSAM for Plans of Action and Milestones (POAM) tracking has been mandatory for all bureaus and offices. All recommendations are assigned a POAM number that is used to track the status of a recommendation, upload artifacts, and determine a final resolution. Bureaus and offices are expected to consistently use CSAM to track program and information system security weaknesses.

A September 23, 2008 memorandum from the Office of the Chief Information Officer (OCIO) titled, *Mandatory Use of the Cyber Security Assessment Management Solution,* specifies:

> "…the mandatory usage and full implementation of the CSAM solution for all of Interior's bureaus and offices for the (1) development of C&A package documentation and to preserve all associated artifacts in CSAM as the official repository, (2) entry and tracking of all weaknesses and associated corrective action plans for IT Security programs and information system accreditation boundaries as part of bureau/office POAM processes consistent with the requirements identified in Interior's POAM Processing Standard, (3) quarterly and annual FISMA performance metrics reporting in conjunction with previously established and relevant information contained in the Departmental Enterprise Architecture Repository (DEAR), and (4) annual IT Security Assessments."

Additional guidance and standards for using CSAM are included in the April 2009 edition of *DOI Certification and Accreditation (C&A) Guide, Using the CSAM Solution, version 2.0*. It states that, "CSAM provides the DOI IT Security Program, Program Officials and IT Security managers with a web-based secure network capability to assess, document, manage and report on the status of IT security risk assessments and implementation of Federal and DOI mandated IT security control standards and policies."

When bureaus and offices resolve weaknesses and report them as completed, they must upload artifacts to support the assertion. We assessed each completed POAM and inspected the artifacts to ensure the appropriate resolution of the recommendation. Incomplete artifacts that did not support closure required additional information and clarification from the appropriate bureau or office.

We reviewed 46 OIG recommendations that bureaus reported as closed prior to May 20, 2009, on POAMs for USGS, BLM, BOR, MMS, NBC, and OS. We concur that 59 percent, or 27 recommendations, were fully resolved.

The following process and implementation weaknesses are affecting management oversight, as well as the full and timely resolution of our recommendations:

1. <u>Artifacts uploaded into CSAM are insufficient to ensure full resolution of recommendations.</u> For example, USGS closed recommendation ISD-EV-GSV-0016-2008 number 6, *"USGS should transition to the ESN architecture as quickly as possible."* The artifacts provided by USGS indicated they had contracted services for making the transition but provided no evidence of the completed transition. The Department's Enterprise Infrastructure Division maintained a list of USGS circuits that were not behind the Enterprise Services Network (ESN) architecture, and even though this information was readily available within the OCIO, the CSD failed to detect and act on the USGS report that the recommendation was fully resolved.

2. <u>Multiple, unrelated recommendations are being recorded under a single POAM number.</u> This practice disallows closure of the POAM unless all recommendations are fully addressed, thus complicating oversight of unresolved recommendations and artificially reducing the number of reported security weaknesses. For example, BOR had recommendation ISD-EV-BOR-0011-2008 number 3, *Lock down external DNS configuration*, recommendation number 6, *ensure that Internet-accessible systems are adequately isolated from internal systems,* and recommendation number 11, *Partition the DNS environment with external DNS servers accessible from the Internet and internal servers for internal network use [and][r]estrict information served from external DNS servers to only what is necessary for Internet-accessible services such as web and ftp*, all

associated with POAM number 10854. We determined recommendations 3 and 11 were resolved; however, since recommendation number 6 was not resolved, the entire POAM must remain open.

3. Artifacts are vague and fail to identify the pertinent information necessary to resolve the recommendation. For example, OS closed recommendation ISD-EV-OSS-0013-2008 number 2, *Develop, test and deploy an effective agency-wide secure workstation baseline using approved security configuration checklists. NIST SP 800-70 (Draft), Security Configuration Checklists Program for IT Products, should be referenced.* The only artifact uploaded into CSAM supporting closure was the DOI IT Security Policy Handbook. We could not identify the agency-wide workstation baseline configuration using that document.

4. Use a Weakness Completion Verification Form (WCVF) to document corrective action related to POAMs. We found many WCVFs were incomplete or did not contain adequate descriptions of the corrective action, while others lacked required signatures. For example, NBC closed recommendation number 26, *Enable auditing on all databases by setting the "AUDIT_TRAIL" to true,* and stated, "verification is attached." We found no attachment. In another example, OS reported recommendation ISD-EV-NBC-0015-2008 numbers 15 and 51 as closed; however, the WCVF did not contain the signature of the lead responder, independent verifier, system owner, or the Chief Information Officer (CIO). We could not determine if any corrective action was taken, or how it was resolved. Departmental oversight must identify and correct these errors.

5. Inconsistent handling of reopened POAM items convolutes oversight, skews management reporting, and hinders the verification of recommendations reported as resolved. For example, MMS reopens POAMs and modifies the status from complete to open if we determine them unresolved, and they use a constant POAM number. In contrast, BLM and BOR reopen recommendations determined unresolved, assign new POAM numbers, and fail to document the transfer within CSAM. Inconsistent handling of reopened POAMs distorts POAM metrics, which reflect closures and new weaknesses. A POAM transfer does not equate to corrective action nor does it reflect management and resolution of IT weaknesses.

6. Recommendations previously reported as unresolved are reported as closed in CSAM. For example, in September 2008, we reported that we were unable to verify closure of USGS recommendation ISD-EV-GSV-0016-2008 number 1, *USGS should immediately deploy effective enterprise-wide intrusion detection and prevention technologies that detect and automatically block malicious activities;* in July 2009 however, we found this recommendation still reported as closed in CSAM without new artifacts to support the assertion. In April 2009, we learned USGS intended to hire an outside contractor to test their intrusion detection system. We sent the USGS CISO an email requesting a copy of

their report when completed. We related our intention to use this report as part of our own verification in order to avoid duplicative testing; however, we did not receive a copy of the report and maintain that the recommendation is not fully resolved.

7. CSAM does not identify the source of POAM weaknesses. Therefore, without completing an extensive manual process, we are unable to determine if CSAM tracks all weaknesses. In the FY 2008 FISMA Evaluation Report, we determined not all weaknesses were tracked on POAMs and not all potential sources were considered. The source information is necessary to track weaknesses from identification through the management and resolution process.

Summary of Sampled Recommendations

A recommendation is successfully resolved when the artifacts, and any additional information obtained, support full resolution of the recommendation. Since the CSAM process to track recommendations correlates to POAM numbers, successful closure of a POAM also results in the recommendation recorded as satisfied.

USGS showed no progress in resolving the OIG recommendations in 2008. They resolved only one of seven recommendations made by the OIG in FY 2007. Artifacts provided by USGS did not provide substantive evidence to support the resolution of recommendations.

BLM also showed no progress in resolving the OIG recommendations in 2008. Thirty-one of 35 recommendations made to BLM in FY 2007 remain unresolved. For this evaluation, BLM reported three recommendations resolved; however, we verified none of the three was fully resolved as they reported. None of the artifacts within CSAM supported closure. We conducted interviews with BLM officials to discuss the status of these recommendations. BLM stated recommendation ISD-EV-BLM-0012 number 16, *At a minimum, a secure workstation baseline STIG should be developed, tested and workstations should at least meet, if not exceed, the baseline STIG,* and recommendation ISD-EV-BLM-0012-2008 number 4, *Secure all Information Access Center offices,* had been transferred to new POAM numbers. We could not determine how CSAM monitored and tracked those recommendations because the appropriate documentation did not exist.

In addition, recommendation ISD-EV-BLM-0012-2008 number 18, *Restrict access to operating systems utilities such as the command prompt and control panel applications, as well as Windows services not required by the employee's job,* was reported resolved on the BLM POAM. CSAM did not contain any supporting artifacts to this assertion. Upon inquiry, BLM determined that they listed the case as closed in error, and they agreed to reopen the recommendation under a new POAM.

BOR demonstrated some progress in resolving past OIG recommendations. Six of the original 13 recommendations remain open following this evaluation. Their practice of combining multiple recommendations in a single POAM impairs oversight and hinders verification of reported closures. BOR reported five recommendations closed, and we verified that three were successfully resolved. Three recommendations, numbers 3, 6, and 11, were associated with a single POAM. Based on the artifacts provided, we confirmed that recommendation number 3, *Lock down external DNS configuration*, and recommendation number 11, *Partition the DNS environment with external DNS servers accessible from the Internet and internal servers for internal network use*, were fully resolved. We do not agree that recommendation number 6, *Ensure that Internet-accessible systems are adequately isolated from internal systems*, was satisfied.

MMS also demonstrated some progress in resolving the OIG recommendations from FY 2007. We made 10 recommendations to MMS, and only one recommendation remains unresolved. We conducted technical testing at the MMS facility in Herndon, VA, on June 9, 2009, to determine the effectiveness of the resolution to recommendation ISD-EV-MMS-0014-2008 number 10, *MMS should fully configure and implement its existing intrusion prevention solution*. MMS demonstrated their ability to detect unannounced network scanning. Recommendation ISD-EV-MMS-0014-2008 number 6 was not fully resolved, and MMS related their intention to separate that recommendation into a new POAM.

NBC demonstrated significant progress in resolving past recommendations from the OIG. Only 14 of the original 59 recommendations from FY 2007 remain open following this evaluation. They reported 23 recommendations closed, and we agreed that 22 were fully resolved. The artifacts that NBC uploaded into CSAM included a thorough description of the corrective action, and the WCVF included screenshots as well as other supporting evidence to support their assertion. Moreover, NBC assigned a single POAM to each recommendation; therefore, closures of recommendations and POAMs were easily monitored.

During this evaluation, however, we discovered that the majority of NBC recommendations are tracked under OS POAM numbers. Combining OS and NBC recommendations on the same POAM introduces challenges to the tracking system and affects management oversight. Reporting POAMs under OS rather than NBC may be misleading and may artificially lower NBC's reported security weaknesses.

In addition, OS failed to implement their own process for managing recommendations consistently within CSAM. OS had 37 FY 2007 recommendations and following this evaluation, 24 remain open. They reported 10 completed recommendations and we confirmed the closure of three. We found artifacts uploaded into CSAM were incomplete, inconsistent, and frequently did not address the recommendation. Recommendation ISD-EV-OSS-0013-2008 number 1, *Design and implement an effective agency-wide Continuous Monitoring program as specified by NIST*

SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, was reported as complete but lacked the appropriate artifacts to support closure. Continuous monitoring is a critical component of the Department's information security program and is a FISMA requirement. The artifact submitted did not define an effective agency-wide continuous monitoring program. The policy submitted was clearly applicable to NBC and OS, but did not provide policy or procedures to any other bureau or office. In fact, the OS artifact was the same artifact submitted by NBC in support of the recommendation for NBC to implement continuous monitoring.

Moreover, recommendation number 37 from our prior report ISD- EV-OSS-0013-2008, *Design and use consistent error handling mechanisms that are capable of handling any user input to the web application without displaying extensive error messages to users* had conflicting information in CSAM that does not support closure of this recommendation.
We pulled a review of this POAM from CSAM on May 20, 2009, that revealed the following:

Detailed Weakness Description	Create Date	Planned Start Date	Actual Start Date	Planned Finish Date	Actual Finish Date	Status	Approval Status
ISD- EV-OSS-0013-2008: (37)Design and use consistent error handling mechanisms that are capable of handling any user input to the web application without displaying extensive error messages to users.	2/21/09	2/21/09	5/12/08	3/23/09	8/29/08	In Progress	POAM Close Requested

As seen in the chart above, the actual finish date comes chronologically before the create date. Documentation within CSAM lacks adequate details for us to determine and verify the status.

Generally, the bureaus and offices are not resolving the OIG recommendations in a timely manner. IT implemented CSAM in 2008 to manage POAMs, but most bureaus still have not shown material improvement in resolving recommendations, and they have not used CSAM effectively to ensure completion of the corrective action.

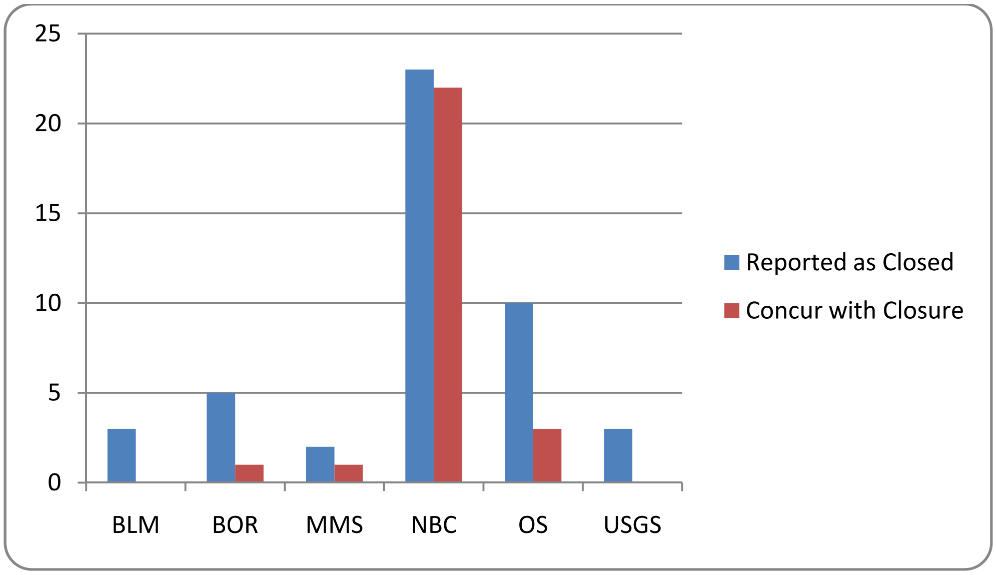


Figure 1: Results of July 2009 Evaluation

Oversight

The Department Manual, part 18, paragraph 18.5(A)1, requires CSD to perform "oversight." In addition, part 375, chapter 19, paragraph 19.8(D)10, requires the Department's CISO to oversee "bureau compliance with Federal and Departmental policies, guidelines, and regulations governing IT security."

Further, the Department's CISO proposed a "Cyber Security Major Reorganization Plan" (Plan) in 2006. The Plan, which was not approved, included a "Compliance and Oversight Division" consisting of 11 fulltime employees, which stated, "The Compliance and Oversight Division provides independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures."

FISMA requires that "significant deficiencies" be reported as a material weakness under the Federal Financial Management Information Act. The Office of Management and Budget (OMB) memorandum, M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, defines significant deficiency as "a weakness in an agency's overall information systems security program or management control structure."

Recommendations

The Department's CSD is responsible for performing oversight, but they lack the necessary resources and expertise to conduct oversight functions such as inspections, technical testing, and monitoring. The lack of oversight is a significant weakness in the Department's overall information systems security program.

To address the deficiencies identified in this report, we recommend consolidation and centralization of common services as a means to improve efficiency, reduce cost, and enhance compliance. Specifically, we recommend the Department:

1. Improve management oversight by adding trained information security inspectors to the Department's CSD and conducting periodic inspections and technical control testing. Improve accountability for timely resolution of information security weaknesses.
2. Improve accountability for reporting the accurate status of resolved recommendations and other information technology weaknesses.
3. Standardize procedures for reopening POAMs in CSAM.
4. Include a data field in CSAM to identify the source of the weakness.
5. Require a single POAM item per OIG recommendation.

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

This evaluation reassessed the Department's progress in implementing corrective actions for information security recommendations made by the OIG in FY 2007. In addition, this evaluation assessed the effectiveness of the Department's management oversight of corrective actions.

The evaluation included the use of records obtained from CSAM and other source documents provided by the Department and its bureaus and offices. In order to conduct technical testing, we made site visits to select bureau and office locations. Verification efforts necessitated our office making requests for additional artifacts and conducting interviews.

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

- Reviewed applicable laws, regulations, OMB guidance, National Institute of Standards and Technology standards, and Department policies.

- Reviewed documentation and supporting artifacts, such as screenshots, scanned documents, WCVFs, POAMs, and photographs provided by the bureaus and offices in support of closure of recommendations.

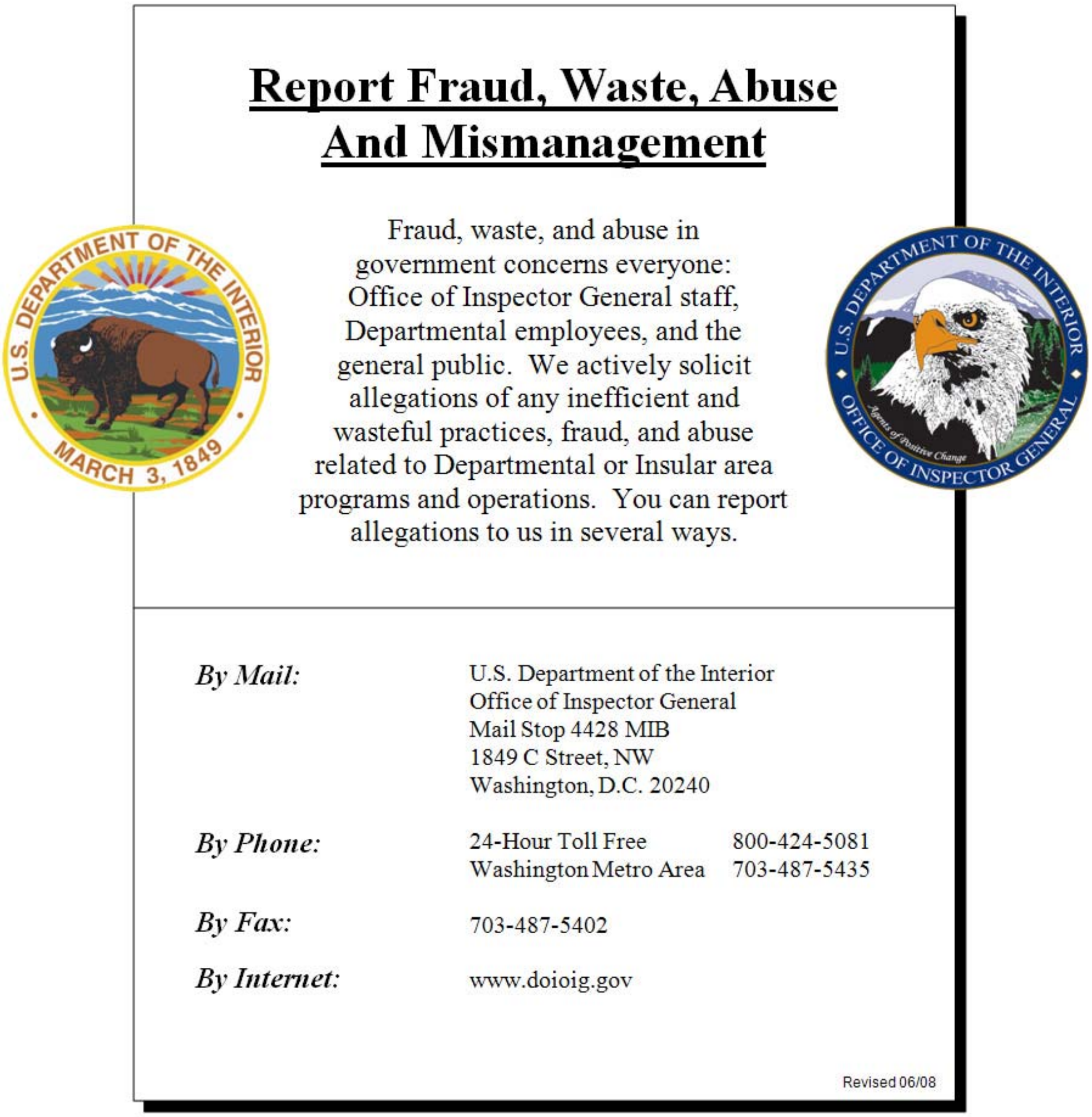
- Interviewed the Department, bureau, and office IT personnel.

- Performed on-site inspections of bureau and office locations.

- Performed technical testing as needed to verify closed recommendations.

Other Related Coverage

The OIG issued a report, *Compilation of Information Technology Challenges at the DOI*, dated May 2008 that documented the need for sweeping reform in the Department's management of IT. In addition, our office issued the annual FISMA evaluation report in September 2008. The FISMA report documented the organizational challenges and inefficiencies that impeded information security across the Department.



Report Fraud, Waste, Abuse And Mismanagement

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

By Mail:	U.S. Department of the Interior Office of Inspector General Mail Stop 4428 MIB 1849 C Street, NW Washington, D.C. 20240	
By Phone:	24-Hour Toll Free Washington Metro Area	800-424-5081 703-487-5435
By Fax:	703-487-5402	
By Internet:	www.doioig.gov	

Revised 06/08