IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELOUISE PEPION COBELL, et al.,

Plaintiffs,

v.

GALE NORTON, et al.,

Defendants.

)
)
)
)
)
)
)
)
)
)
)
)

No. 1:96CV01285
(Judge Lamberth)

FILED UNDER SEAL

**DEFENDANTS' NOTICE OF FILING OF THE DEPARTMENT OF THE INTERIOR'S
FISCAL YEAR 2005 FISMA REPORTS AND IG REPORT ON THE POA&M PROCESS**

Defendants hereby submit the 2005 Federal Information Security Management Act

("FISMA") reports from the Secretary of the Department of the Interior and the Department of

the Interior's Office of the Inspector General ("OIG"), as well as the proposed redactions thereto.

In addition, Defendants submit the OIG's report concerning the Department of the Interior's Plan

of Actions and Milestones ("POA&M") process. Defendants submit the reports and proposed

redactions pursuant to the Court's April 22, 2005 Protective Order.

Dated: November 17, 2005   Respectfully submitted,

ROBERT McCALLUM, JR.
Associate Attorney General
PETER D. KEISLER
Assistant Attorney General
STUART E. SCHIFFER
Deputy Assistant Attorney General
J. CHRISTOPHER KOHN
Director

/s/ Robert E. Kirschman, Jr.
ROBERT E. KIRSCHMAN, JR.
(D.C. Bar No. 406635)
Assistant Director
GLENN D. GILLETT
Trial Attorney
Commercial Litigation Branch
Civil Division
P.O. Box 875
Ben Franklin Station
Washington, D.C. 20044-0875
Telephone: (202) 307-0494
Facsimile: (202) 514-7162

<u>CERTIFICATE OF SERVICE</u>

I hereby certify that, on November 17, 2005 a copy of the foregoing *Defendants' Notice of Filing of the Department of the Interior's Fiscal Year 2005 FISMA Reports and IG Report on the POA&M Process* in PDF Format on CD was served upon:

Dennis M Gingold, Esq.
Mark K. Brown, Esq.
Elliot Levitas, Esq
607 - 14th Street, NW, 9th Flr.
Washington, DC 20005

and, without under seal attachments, on the following who is not registered for Electronic Case Filing, by facsimile:

Earl Old Person (*Pro se*)
Blackfeet Tribe
P.O. Box 850
Browning, MT 59417
Fax (406) 338-7530

    /s/ Kevin P. Kingston
     Kevin P. Kingston

THE SECRETARY OF THE INTERIOR

WASHINGTON

OCT 1 4 2005

The Honorable Joshua B. Bolten
Director
Executive Office of the President
Office of Management and Budget
Washington, D.C. 20503

Dear Mr. Bolten:

The Department of the Interior (DOI) provides the enclosed information technology (IT) compliance report, prepared using the guidance contained in the Office of Management and Budget (OMB) memorandum M-05-15, *FY 2005 Reporting Instructions for the Federal Information Security Management Act*, June 13, 2005. The annual report includes both the views of the agency Chief Information Officer (CIO) and the Inspector General (IG), a discussion on the differences between those perspectives, and the new privacy requirements.

Interior made significant progress in improving its overall security posture in FY 2005, in spite of the extraordinary burden placed on Interior by the ongoing *Cobell v. Norton* litigation. In the *Cobell* case, we produced over 4 ½ million pages of documentation, and testified throughout a 59 day evidentiary hearing. The significant demands on us to respond to the court impacted the annual FISMA evaluation, causing delays and limitations for both the CIO's staff and the IG's staff.

I would like to highlight the following progress made in FY 2005:

- DOI made progress toward consolidating 13 networks into a single Departmental Enterprise Services Network (ESN). Three remaining bureau networks are targeted for consolidation this month.
- The ESN architecture includes robust network perimeter security controls and enables Interior to manage perimeter controls more consistently, effectively, and cost-efficiently.
- The Department is maintaining a continuous monitoring program as part of the Certification and Accreditation (C&A) processes. This includes:
  - independent third-party review of C&A packages,
  - routine automated vulnerability scanning and remediation of identified weaknesses,
  - internal and external penetration testing of networks and major applications, and
  - an improved Plan of Actions and Milestones (POA&M) system implementing the changes recommended by the IG.
- Interior initiated state-of-the-art penetration testing, independently conducted by the Office of IG, for DOI's bureaus and offices. The enhanced monitoring program provided critical information needed to prioritize further improvements to our operational security posture.

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 1 of 37

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

- OMB rated DOI's Enterprise Architecture (EA) the highest among the 25 EA programs reviewed. The DOI EA was noted as incorporating a security standards profile, and aligned to the Technical Reference Model.
- The Department entered into an agreement with USALearning.gov to deliver a standardized curriculum for individuals with significant IT security roles.
- The DOI CIO contracted an independent IT security assessment to evaluate DOI against the myriad of security policies and guidance. We are pleased to report 3.63 maturity level out of 5 from this assessment.

IT security has been, and will continue to be, one of my highest priorities, as evidenced by the major improvements made throughout the DOI this past year. This progress builds on accomplishments of the past. In June 2004, the IG concluded "the DOI POA&M process is effective and satisfies the pertinent Federal guidance." The IG's FY 2004 report considered Interior's C&A process as being satisfactory. The percentage of IT systems certified and accredited increased from 83 percent for FY 2004 to over 98 percent in FY 2005. With better accountability and standardization, DOI, and ultimately the taxpayers, avoided $17 million in C&A costs. We are pleased with the return on the investment OMB and Congress authorized in our FY 2004 budget and sustained in FY 2005. In FY 2005, the IG appropriately raised the bar for evaluating the security program, based on DOI's increased maturity in the program. I support his efforts and his resources have increased to enable measurements against these higher standards. Our collaborative efforts in monitoring our systems through exhaustive penetration testing illustrate our commitment to maintaining a constantly improving C&A process.

We recognize that the C&A process is not perfect, particularly in light of the many new or revised standards published by National Institute of Standards and Technology (NIST) within the past year, some of which are still in draft. We recognize that C&A is primarily a process of risk management, requiring application of considerable subjective judgment. Without clear criteria for reporting, the ambiguity leads to subjectivity based on individual perspectives. In preparing this year's report, I am struck by how strongly this subjectivity is impacted by the role of two key executives at DOI: the IG and the CIO. Your guidance for the FY 2005 report asks that I include an analysis of the differences between the CIO's report and the IG's. I hope you will find this useful in reducing the ambiguity of future reporting, and to more fully understand the perspectives presented. Through consistent reporting standards, we can arrive at a fair comparison of government security progress and deficiencies, and achieve or exceed the benchmark leading to adequate security.

I understand the IG's opinion that the IT security at DOI is not perfect, that risks and vulnerabilities still remain and improvements need to be made. From this he concludes DOI has significant weaknesses in complying with FISMA. From this perspective, the IG tempered the scores on his report by any weakness seen:

- where a C&A package did not contain all required elements clearly presented. it was not counted as a valid package;
- problems in the POA&M process were included in the IG report dated September 23, 2005, even though subsequently corrected, because the corrections had not been verified by the OIG; and
- any deviations from policy or procedures were reported as an inconsistent and ineffective policy overall.

The IG's perspective can be supported by the language of the OMB and NIST requirements. It is consistent with the IG's role of being DOI's watch dog – who clearly needs to warn of any potential risks, regardless of the weight or costs. The CIO believes the IG's responses to several of the questions in the FY 2005 reporting template exceed the basic requirements of FISMA and do not take into account improvements made during the year in response to the testing the IG conducted.

I have confidence in the CIO's opinion that, while IT security at DOI is not perfect, risks and vulnerabilities still remain, and improvements need to be made, nonetheless, the policies and processes to address those risks are adequate, improvements have been and will continue to be made, and therefore. DOI substantially complies with FISMA. From this perspective, when weaknesses are found, DOI corrects them and takes credit for having done so. Based on extensive reviews of the IT security program, the CIO believes these corrective actions have generally been completed, sufficient to meet the basic requirements of FISMA. As required by FISMA, remaining problems are being addressed through the POA&M process.

The CIO perspective is clearly supported by the language of the OMB and NIST requirements. It is also consistent with the CIO's role, which requires him to balance risks to DOI's information assets with the costs to address those risks. The CIO also appropriately relies on the determinations of competent accountable officials, including the IG. The CIO points out that Interior was successful in thwarting over 353 million potential incidents in contrast to only 33 incidents that could not be prevented, as reported during our last quarterly reporting period. None of the successful incidents have resulted in any known compromise of sensitive data.

I ask for your assistance in determining where, between these two perspectives, your intent in measuring FISMA compliance lies. This determination has significant funding and operational implications to DOI, in addition to arriving at a credible determination of "adequate" security. I am obviously concerned about the cost implications of eliminating every defect when risks are not significant to security or operations.
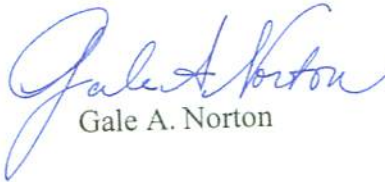
We have clearly demonstrated a commitment to maintaining an effective IT security program at funding levels commensurate with the value of Interior's IT assets. I remain committed to continued improvements in DOI's IT security posture, including improvements to the C&A and POA&M processes. As you are aware, continued funding

Mr. Joshua B. Bolton

is critical to maintain the accreditation status of Interior's IT systems, including the continuous monitoring requirement.

While I believe we are substantially in compliance with FISMA, I request your determination in the interpretation of your requirements.

Sincerely,

Gale A. Norton

Enclosures

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 4 of 37

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

Section B: Chief Information Officer. Questions 1, 2, 3, and 4.

Agency Name: U.S. Department of the Interior

Question 1 and 2

1. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of information systems used or operated by your agency, and the number of information systems used or operated by a contractor of your agency or other organization on behalf of your agency.

   Note: Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

   To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
   1) Continue to use NIST Special Publication 800-26, or,
   2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

   Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

   FIPS 199, a Federal information processing standard, was published in February 2004. If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain below in item (d.).

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the Total Number of Systems, identify the number of systems which have: a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year. Contingency planning is a requirement for certification and accreditation, with annual contingency plan testing required thereafter. If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain.

| | | Question 1 | | | | | | Question 2 | | | | |
| | | a. FY 05 Agency Systems | | b. FY 05 Contractor Systems | | c. FY 05 Total Number of Systems | | a. Number of systems certified and accredited | | b. Number of systems for which security controls have been tested and evaluated in the last year | | c. Number of systems for which contingency plans have been tested in accordance with policy and guidance | |
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
BIA	High	12	12	3	3	15	15	14	93.3%	14	93.3%	14	93.3%
	Moderate	20	20	2	2	22	22	22	100.0%	22	100.0%	22	100.0%
	Low	3	3			3	3	3	100.0%	3	100.0%	3	100.0%
	Not Categorized					0	0						
	Sub-total	35	35	5	5	40	40	39	97.5%	39	97.5%	39	97.5%
BLM	High					0	0						
	Moderate	23	23			23	23	23	100.0%	23	100.0%	23	100.0%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	23	23	0	0	23	23	23	100.0%	23	100.0%	23	100.0%
BOR	High	1	1			1	1	1	100.0%	1	100.0%	1	100.0%
	Moderate	22	22			22	22	22	100.0%	22	100.0%	21	95.5%
	Low	12	12			12	12	12	100.0%	12	100.0%	12	100.0%
	Not Categorized					0	0						
	Sub-total	35	35	0	0	35	35	35	100.0%	35	100.0%	34	97.1%
FWS	High	1	1			1	1	1	100.0%	1	100.0%	1	100.0%
	Moderate	10	10			10	10	10	100.0%	9	90.0%	10	100.0%
	Low	1	1			1	1	1	100.0%	1	100.0%	1	100.0%
	Not Categorized					0	0						
	Sub-total	12	12	0	0	12	12	12	100.0%	11	91.7%	12	100.0%
MMS	High					0	0						
	Moderate	5	5			5	5	5	100.0%	5	100.0%	5	100.0%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	5	5	0	0	5	5	5	100.0%	5	100.0%	5	100.0%
NBC	High	1	1			1	1	1	100.0%	1	100.0%	1	100.0%
	Moderate	6	6			6	6	6	100.0%	6	100.0%	6	100.0%
	Low	1	1	1	1	2	2	1	50.0%	1	50.0%	1	50.0%
	Not Categorized					0	0						
	Sub-total	8	8	1	1	9	9	8	88.9%	8	88.9%	8	88.9%
NPS	High					0	0						
	Moderate	5	5			5	5	4	80.0%	4	80.0%	4	80.0%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	5	5	0	0	5	5	4	80.0%	4	80.0%	4	80.0%
OHA	High	1	1			1	1	1	100.0%	1	100.0%	1	100.0%
	Moderate					0	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	1	1	0	0	1	1	1	100.0%	1	100.0%	1	100.0%
OS	High	3	3	1	1	4	4	4	100.0%	4	100.0%	4	100.0%
	Moderate	10	10	2	2	12	12	12	100.0%	12	100.0%	11	91.7%
	Low					0	0						

	Not Categorized					0	0						
	Sub-total	13	13	3	3	16	16	16	100.0%	16	100.0%	15	93.8%
OSM	High					0	0						
	Moderate	4	4			4	4	4	100.0%	4	100.0%	1	25.0%
	Low	1	1			1	1	1	100.0%	1	100.0%	0	0.0%
	Not Categorized					0	0						
	Sub-total	5	5	0	0	5	5	5	100.0%	5	100.0%	1	20.0%
OST	High					0	0						
	Moderate	1	1	1	1	2	2	2	100.0%	2	100.0%	2	100.0%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	1	1	1	1	2	2	2	100.0%	2	100.0%	2	100.0%
SOL	High					0	0						
	Moderate	1	1			1	1	1	100.0%	1	100.0%	0	0.0%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	1	1	0	0	1	1	1	100.0%	1	100.0%	0	0.0%
USGS	High	2	2			2	2	2	100.0%	2	100.0%	2	100.0%
	Moderate	10	10			10	10	10	100.0%	9	90.0%	10	100.0%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	12	12	0	0	12	12	12	100.0%	11	91.7%	12	100.0%
Agency Totals	High	21	21	4	4	25	25	24	96.0%	24	96.0%	24	96.0%
	Moderate	117	117	5	5	122	122	121	99.2%	119	97.5%	115	94.3%
	Low	18	18	1	1	19	19	18	94.7%	18	94.7%	17	89.5%
	Not Categorized	0	0	0	0	0	0	0		0		0	
	Total	156	156	10	10	166	166	163	98.2%	161	97.0%	156	94.0%

1.d.	If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain: The CIO's responses to these questions are appropriately categorized by the FIPS Pub 199 risk impact levels as required. The OIG does not recognize these documented risk impact levels as they have asserted that the method prescribed by the Department's Asset Valuation Guide (AVG) is not compliant with NIST FIPS Pub 199. However, the OIG has indicated that they are in agreement with the OCIO that the existing method used by Interior typically meets or exceeds the provisional impact ratings that would be obtained by leveraging the NIST SP 800-60 ratings for information types derived from the Business Reference Model (BRM) and Federal Enterprise Architecture (FEA) as well as if Interior even elevated those impact ratings through subsequent application of the FIPS
2.d.	If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain: 156 systems of the 166 identified systems have undergone contingency testing during FY 05. Assurances have been made by the bureaus and offices to complete contingency testing for the remaining systems. Of the 10 systems not tested this year, most of them have been tested in previous years.

Question 3

Agencies must implement the recommended security controls in NIST Special Publication 800-53.

3.a.	Do you have a plan in place to fully implement the security controls recommended in NIST Special Publication 800-53? Yes or No.	Yes
3.b.	Have you begun to implement the security controls recommended in NIST Special Publication 800-53? Yes or No	No

Question 4

Incident Detection Capabilities.

4.a.	What tools, techniques, technologies, etc., does the agency use for incident detection? Response: See "Attachment A"
4.b.	How many systems (or networks of systems) are protected using the tools, techniques and technologies described above? Response: 166

Information gathered in this question will be forwarded to the Department of Homeland Security for validation.

For each category of incident listed: identify the total number of successful incidents in FY 05, the number of incidents reported to US-CERT, and the number reported to law enforcement.   If your agency considers another category of incident type to be high priority, include this information in category e., "Other". If appropriate or necessary, include comments in the area provided below.

Type of Incident:	5. Number of Incidents, by category:		
	Reported internally	Reported to US-CERT	Reported to law enforcement
	Number of Incidents	Number of Incidents	Number of Incidents
a. Unauthorized Access	23	22	2
b. Denial of Service (DoS)	2	2	0
c. Malicious Code	191	171	1
d. Improper Usage	34	28	4
e. Other	36	28	3
Totals:	286	251	10

Comments:

6. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?
Yes or No.

a. Total number of employees in FY05	b. Number of employees that received IT security awareness training in FY 05. as described in NIST Special Publication 800-50 "Building an Information Technology Security Awareness and Training Program" (October 2003)		c. Total number of employees with significant IT security responsibilities	d. Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)		Total costs for providing IT security training in FY05 (in $'s)
	Number	Percentage		Number	Percentage	
84,159	82.848	98.44%	2611	1736	66.49%	$1,340,487

6.e.	Briefly describe the training provided in b. and d: Employees are trained by using a comprehensive DOI University online system. The training covers a broad range of IT security subjects including, access controls, passwords, malicious code (viruses), DOI Policy and Federal Regulations. Central reporting is built into the system and provides compliance tracking by bureaus and offices. Specialized training for those with "significant security responsibilities" includes certification courses. industry and vendor training classes; internal briefings and awareness seminars (for designated authorities, senior management, technical staff, and security representatives; DOI IT security team meeting training sessions; and online continuing education.

Comments: DOI has taken steps to enhance IT security training in FY 2005 by contracting with USALearning gov to provide role based training for bureaus and offices. The curriculum provides specialized training modules geared towards DAA's. system owners, ISSO's, and network, database, and system administrators. This will undoubtably raise Interior's compliance levels with respect to training those "with significant IT security responsibilities". In FY 2005, the CIO and CISO provided C&A training to the Secretary and other senior management officials having DAA responsibilities. This role-based training included a review of the C&A process and the responsibilities of the DAAs, Certifying Officials, ISSOs and other individuals assigned C&A roles and responsibilities. The Bureau IT Security Managers (BITSMs) are constantly engaging in external training and certification. Over 80 IT staff, including BITSMs and some of their security staff. have achieved certifications as Certified Information Systems Security Professionals (CISSP). In addition, eight employees recently achieved certification as Certification and Accreditation Professionals (CAP). These eight indivuduals are among the first in the country to receive such certification. Sec

*** It is important to note that the 84,159 reported in §a. includes ALL employees and contractors (per instructions). A percentag

Question 7

Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?
Yes or No.   Yes

Question 8

8.a.	Is there an agency wide security configuration policy? Yes or No.	Yes

Comments: Policy Directive Issued by the Office of the Chief Information Officer

8.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	Addressed in agencywide policy? Yes, No, or N/A.	Do any agency systems run this software? Yes or No.	Approximate the extent of implementation of the security configuration policy on the systems running the software. Response choices include: - Rarely, or, on approximately 0-50% of the systems running this software - Sometimes, or on approximately 51-70% of the systems running this software - Frequently, or on approximately 71-80% of the systems running this software - Mostly, or on approximately 81-95% of the systems running this software - Almost Always, or on approximately 96-100% of the systems running this software
Windows	Yes	Yes	- Frequently, or on approximately 71-80% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Windows	Yes	Yes	- Sometimes, or on approximately 51-70% of the systems running this software
Windows	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Solaris	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software
Linux	Yes	Yes	- Rarely, or on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Rarely, or on approximately 0-50% of the systems running this software
Oracle	Yes	Yes	- Sometimes, or on approximately 51-70% of the systems running this software
Other. Specify: IIS, SQL Svr, Other Windows, HP MPE, MAC, Novell, AIX	Yes	Yes	- Mostly, or on approximately 81-95% of the systems running this software

Comments: Interior has established approved security configuration standards in the form of Security Technical Implementation Guides (STIGs). Interior's policy allows for bureaus to define, document, approve, and implement their own STIGs which many have done, or implement Departmental STIGs. The CIO and IG differ in their perspectives with respect to the level of policy compliance and STIG implementation by Interior's bureaus and offices due to a misunderstanding between our respective interpretations of what the FISMA questions are asking and the IG's understanding of Interior's policy. The OIG appears to be of the opinion that bureaus must implement the Departmental STIGs and does not reflect the same credit and degree of compliance with respect to bureau-level implementation of STIGs as the CIO's FISMA report. The OIG has acknowledged in their evaluation report that bureaus frequently have their own STIGs which they implement.

Question 9

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
9.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: The IG's FISMA report differs from the CIO's with respect to question 9.b based on their observation that in 8 of 12 instances the OIG was not notified. Unlike many other response choices for other questions in the FISMA template, this is a binary answer and does not enable a more appropriate selection that would identify the relative frequency where such incidents are in fact reported to the IG or consideration of circumstances preventing full compliance with established external reporting procedures. The CIO believes that appropriate policies and procedures are in place and that there may be other mitigating circumstances that may have precluded adherence to these general procedures.

Question 10

10.a.	Has the agency documented in its security policies special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)? Yes or No.	Yes
10.b.	If the answer to 10 a. is "Yes," briefly describe the documented procedures. These special procedures could include more frequent control tests & evaluations, specific configuration requirements, additional monitoring, or specialized training.	

Response: Interior develops, maintains, and updates IT security policies and Security Technical Implementation Guides (STIGs) to respond to emerging threats and technologies. As part of DOI's Certification and Accreditation (C&A) continuous monitoring process, systems are routinely assessed to identify and correct weaknesses resulting from newly discovered vulnerabilities. Depending on the nature of the emerging threat or technology, more frequent control testing, specialized training for network or system administrators, additional monitoring, or application of STIGs to ensure specific configuration requirements are met may be required for systems. Such requirements are typically specified through Departmental or bureau policy or standards, and Designated Approving Authorities have the discretion to identify additional system specific security control requirements depending on agency, risk, threat, and technological factors.

Comments:

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 9 of 37

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

Attachment A: §4.a. Incident Detection Capabilities.

Response:

Incident Response Tools and Technology

The Department of the Interior Computer Incident Response Capability (DOI-CIRC) uses a variety of tools to classify, track, and report IT security incidents. E-mail, telephone, and collaborative communication are the predominate methods used to alert, track and manage incidents. In a network-wide alert, e-mail is used to notify all employees. IT staff, IT security professionals, or other well-defined groups of an ongoing security incident and the appropriate action to be followed. The incident response teams use e-mail and other collaborative communication tools to exchange information on an incident through the seven stages of remediation: detection, classification, containment, reporting, investigation, recovery, and closing. Web technology is used to inform employees of the action to be followed in reporting an incident, as well as to maintain a permanent record of the incident in a response database.

A variety of specialized commercial and freeware tools, scripts, manual and automated procedures are used to collect, review, and correlate IT security system and host logs in the identification and investigation of an IT security incident. For virus and malicious code detection, DOI maintains an Enterprise Anti-Virus/virus protection software contract and uses a variety of commercial host- and network-based intrusion detection capabilities to identify, log, and alert malicious network activities.

Incident Detection

IT security incidents are reported from internal and external sources including: DOI employees, bureau IT security professionals, other federal agencies, and worldwide IT security organizations. As appropriate, DOI-CIRC alerts bureaus of security threats to the Department's network infrastructure and tracks the security alert from alert and classification through remediation and closing. In the initial phases of an alert, a security incident handler is assigned to track, record, and communicate information about the incident. Incidents classified high or medium are reported to the Bureau IT Security Manager (BITSM) and DOI-CIRC within two hours or two days, respectively. Incidents classified as low are reported to DOI-CIRC monthly.

Perimeter and Wide-Area Network Incident Detection

Logging is enabled on all security devices, including routers, network- and host-based firewalls, intrusion detection/prevention and other security systems. These security devices are configured to log access from, and egress to, the public Internet. In some environments, wide-are-network routers are similarly configured to log events between internal network segments.

Network- and host-based event logs are routinely monitored for indication of significant security events and potential malicious activity. Security events include network intrusions, scans, denial of service attacks, worms, and unauthorized access to network integrated devices in the DOI wide-are-network infrastructure. Client initiated (egress) access is routinely reviewed to detect

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

security incidents, including attempted propagation of malicious code from an infected or otherwise compromised host, inappropriate use of Internet services, or events including misconfigured internal hosts.

Internal Incident Detection and Alerting

As part of the IT Security Program, each bureau operates a computer security incident team to work closely with the BITSM and DOI-CIRC in the classification, containment, reporting, and remediation of identified security incidents. Any event classified as a security incident is reported to DOI-CIRC and is addressed using the standard methodology presented in the Department of the Interior Computer Security Incident Response Handbook.

Internal security events are reported to the bureau incident response team or DOI-CIRC for assignment of an event manager to track the event and log all action with the appropriate authorities. Viruses and malicious code are detected using anti-virus software technology deployed with individual workstations, mail servers, and SMTP e-mail gateway servers. Detection and quarantine/removal of malicious code is considered a security event and reported monthly to DOI. An infected message or other malicious payload inadvertently launched at the workstation is reported as a security incident.

External Reporting of Security Incidents

DOI and its bureaus maintain Internet e-mail accounts for reporting possible security incidents originating from DOI computer systems. These reports are delivered to the BITSM and computer security incident response team (CSIRT). The e-mail address for reporting security incidents to DOI is incident@circ.doi.gov.

Discussion of Differences between CIO and IG Sections

Introduction

Each year. the Chief Information Officer (CIO) and the Inspector General (IG) complete different sections of the annual Federal Information Security Management Act (FISMA) report. The sections represent the respective viewpoints of the Office of the Chief Information Officer (OCIO) and Office of the Inspector General (OIG) with regard to the degree to which Interior's Information Technology (IT) Security Program is compliant with FISMA.

This document provides a gap analysis between the OIG's characterization of Interior's FISMA compliance, as documented in their responses to Section C of the FY 2005 annual report and their Annual Evaluation of the Department of the Interior Information Security Program (Report No. NSM-EV-MOI-0013-2005), and the OCIO's characterization, as documented in their draft responses to Section B of the FY 2005 annual report.

The OCIO and OIG worked together to develop and implement a cooperative monitoring agreement on the DOI IT security program. This program, funded by the Department ($1.1 million in FY 2005) and independently conducted by the OIG, provided critical information needed to prioritize further improvements to the DOI operational IT security posture. From quarterly updates provided by the OIG as well as penetration test results, the OCIO was able to promptly take action to correct vulnerabilities. Although additional corrective actions remain from some IG evaluations. many actions were taken immediately, including temporary disconnection from Internet access when warranted. The OCIO appreciates the efforts of the OIG in pointing out weaknesses or vulnerabilities. and has utilized the results to make significant improvements.

The primary difference in the perspectives is a result of the ambiguity in FISMA, and more particularly, differences in the interpretation of the term "adequate security." The CIO believes that the criteria the OIG used exceed the basic requirements of FISMA.

General Comments

The OIG report portrays the DOI OCIO as being uncooperative, requiring the OIG to "modify various testing techniques" and that "information requested from the OCIO was very late in coming," incomplete. or not readable. This does not acknowledge the significant burden placed on already constrained OCIO resources. They were simultaneously engaged in producing over 4 ½ million pages of documentation in response to the court, as well as meeting the new OIG requirements to produce voluminous material in the Cobell litigation (e.g.. CDs and DVDs as well as other information) in support of the OIG FISMA evaluation.

The effort by the OIG to obtain. load, and inspect copies of bureau hardened and secured baseline operating system and database images represented a significant new workload.

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 12 of 37

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

The varying results (e.g., copies of default manufacturer provided images as opposed to hardened and secure baseline images) in obtaining these copies were partially attributed to insufficient advance notice for the new requirement and insufficient time to clearly communicate what was expected.

The OIG report did not indicate that, for FY 2005, the OCIO provided funding to the OIG to participate with the Department in a collaborative but independent fashion to augment our compliance program. The report does not mention the significant progress in implementing corrective actions for weaknesses identified in the penetration tests performed by the OIG as part of the compliance program funded by the OCIO.

In summary, the executive summary of the OIG report does not track with the analysis and conclusions provided in the remaining sections of that document. The Department acknowledges areas that need improvement. However the OCIO believes that the OIG's interpretation of several of the questions asked in the FY 2005 FISMA, reporting template exceed the basic requirements of FISMA. For example, the report does not indicate:

- Interior's Certification and Accreditation (C&A) policy, standards, guidelines, processes, and independent compliance reviews is substantially compliant with FISMA and NIST requirements;
- Risk impact level (e.g., Low, Moderate, and High) determinations for confidentiality, integrity, and availability documented in System Security Plans meet or exceed NIST SP 800-60 and FIPS Pub 199 criteria;
- Interior's authoritative Departmental Enterprise Architecture Repository (DEAR) has an accurate inventory of all major information systems;
- Interior's POA&Ms and POA&M process is substantially compliant with OMB requirements;
- Bureaus implemented approved bureau-level STIGs (e.g., security configuration standards) in conformance with Departmental policy; and,
- Substantial C&A training was provided to Department and bureau senior management officials (e.g., Designated Approving Authorities (DAAs) via the MIT forum).

The OCIO believes that, at a minimum, the quality of our C&A process is satisfactory as supported by the following analysis and recommendations. The following analysis represents the perceived differences between the OCIO's and OIG's interpretation of those requirements.

Analysis

The following gap analysis is limited to the areas where the report shows differences of opinion between the CIO and IG. The format used to contrast each area of difference will be identification of the relevant question in Section C used to document the results of the IG's evaluation, and the corresponding question in Section B used to document the results of the CIO's assessment. In responding to each question in the FISMA reporting

template, we believe the objective should be to consider whether Interior's IT security program is adequate when measured against the requirements of FISMA. The level of adequacy would include the degree to which Interior has substantially demonstrated compliance with Federal laws, regulations, and standards such as Memoranda and Circulars issued by the Office of Management and Budget (OMB) and Federal Information Processing Standard Publications (FIPS Pubs) and Special Publications (SPs) issued by the National Institute of Standards and Technology (NIST). Adequacy should be characterized by the degree to which:

- Interior has adequate IT security policies,
- Processes and procedures are in place to implement those policies, and
- Programs and systems have been sufficiently tested to ensure that agreed upon security controls, as approved by senior management officials (e.g., Designated Approving Authorities (DAAs)) and as documented in security plans, are functioning as intended.

IG's FISMA Section C Response	Questions 1a thru 1c and 2a thru 2c
CIOs's FISMA Section B Response	Questions 1a thru 1c and 2a thru 2c
Difference	For each question, actual performance in FY 2005 by risk impact level and bureau are expected to be identified. The FISMA template provides a heading for the second column for these questions that reads "FIPS 199 Risk Impact Level." Potential risk impact ratings (e.g., High, Moderate, or Low) for Confidentiality, Integrity, and Availability (CIA) and the resulting overall security categorization of IT systems (e.g., the high-water mark of the impact ratings for CIA) for each system are documented in their respective System Security Plans (SSPs). The CIO responses to these FISMA questions are identified by the documented FIPS 199 Risk Impact Levels as required. The OIG does not recognize these documented risk impact levels as they have asserted that the method prescribed by the Department's Asset Valuation Guide (AVG) is not compliant with NIST FIPS Pub 199. However, the OIG also indicated the existing method used by Interior typically meets or exceeds the provisional impact ratings that would be obtained by using the NIST SP 800-60 and FIPS Pub 199 ratings.
Discussion	The NIST standards provide for flexibility for agencies to define their own common data and information types. The standards also provide guidance for determining risk impact levels using those types, considering other factors unique to each agency, as long as the resulting sensitivity ratings equal or exceed the minimum thresholds and specifications prescribed by NIST. As long as agencies:

- identify, select, implement, and test minimum mandatory management, operational, and technical security controls based on the security categorization of each system;
- risk impact levels equal or exceed minimum expected sensitivity ratings as identified by the provisional ratings contained for similar data and information types specified in NIST SP 800-60; and
- security controls are tailored to individual ratings for CIA, as specified by the draft NIST FIPS Pub 200 and the related NIST SP 800-53;

then the agency has demonstrated a consistent and adequate methodology used to determine risk impact ratings for IT systems. Agencies aren't expected to have implemented NIST FIPS Pub 200 and SP 800-53 until one year following the final release of FIPS Pub 200, currently still in draft.

In an earlier meeting with the OIG, the OCIO was informed that the sensitivity ratings and security categorizations were not documented in any of the C&A packages (e.g., in the SSP or the Risk Assessment report). The OCIO reviewed the C&A packages in question and found the information documented in the SSPs. In a follow-up conversation with the OIG, the OCIO was informed that the real issue was related to inconsistencies between what was documented in the AVGs compared to the SSPs. Although the AVG serves a useful purpose as a tool for the System Owner to develop a recommendation for the ratings to be considered by the DAA, it does not serve as the documentation for the final determination. The final sensitivity ratings for CIA, the overall security categorization and the agreed upon security controls are documented in the DAA-approved final SSP.

The OIG report reflects a more narrow interpretation of the NIST standards which we believe is inconsistent in their recognition that Interior's existing process results in sensitivity and impact determinations which equal or exceed the provisional impact ratings identified in NIST SP 800-60, which inherently considers the NIST FIPS Pub 199 minimum impact rating determinations. This interpretation does not recognize the agency's discretion in identifying additional criteria and requirements which may result in higher impact levels being assigned to systems.

The OCIO recognizes the need to reevaluate the existing process to ensure that systems are not overly categorized in terms of data and information sensitivity and impact ratings. This is particularly important as there is an associated burden and cost implication to

| | implement the operational, and technical security controls appropriate to these ratings.

The OIG appeared to base their conclusion on interviews with individuals as to whether they had followed NIST FIPS Pub 199 in determining these ratings. The individuals were not familiar with that NIST publication and had indicated that they had used the AVG process. The OIG did not provide recognition in their report that the sensitivity determinations had been based on consistent application of the AVG methodology. They also did not indicate that the AVG process resulted in sensitivity determinations lower than what they would expect from the FIPS Pub 199 process alone. There is no requirement that individuals be familiar with the specific NIST FIPS Pub 199 reference (e.g.. recognize the name or title of a reference). if they are following an agency-prescribed process that incorporates those requirements.
The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with these questions exceed the essential requirements of FISMA. |
|---|---|

IG's FISMA Section C Response	Question 3b
CIOs's FISMA Section B Response	No corresponding question(s)
Difference	Question 3b asks the IG to evaluate the degree to which "The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including identification of the interfaces between each such system and all other systems or networks. including those not operated by or under the control of the agency." The IG's response characterizes Interior's inventory of **"major information systems"** as "approximately 81-95% complete" while the CIO remains confident that the Department Enterprise Architecture Repository (DEAR), the authoritative repository for IT system inventory, contains an accurate inventory of the Department's major information systems.
Discussion	The OIG's evaluation does not identify any specific discrepancies with respect to the Department's inventory of major information systems necessary to substantiate their response characterizing Interior's inventory at anything less than 100%.

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 16 of 37

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

	The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA.

IG's FISMA Section C Response	Question 4a
CIOs's FISMA Section B Response	No corresponding question(s)
Difference	Question 4a asks the IG to select from one of several response categories with respect to the degree to which "The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency." The OIG selected the response category of "Sometimes. for example, approximately 51-70% of the time" and in their comments on the FISMA response indicated that they "did not determine the amount of unreported IT security weaknesses that were not included in the POA&Ms". The OCIO has no basis to suggest that weaknesses captured on POA&Ms are anything less than the highest response category option of "Almost Always, for example, approximately 96-100% of the time."
Discussion	In FY 2005. the DOI POA&M process tracked 2,895 weaknesses. The OIG acknowledges that DOI captures up to 95% of OIG identified weaknesses. The Department has very formal procedures in place. particularly for the financial audit, to ensure 100% of weaknesses are recorded in system POA&Ms. The OCIO is at a loss to determine where another 1.000+ (this number would be based on OIG current response indicating that the Department incorporates known weaknesses only "Sometimes. for example, approximately 51-70% of the time") weaknesses should be derived. It appears that there is substantial agreement on the nature and number of weaknesses and the POA&M report takes exception to methods of resolution.
	The remaining findings are based upon the OIG report for the DOI POA&M process that questions the methods by which POA&M items are closed and the nature of prioritization. In response to OIG concerns, the DOI CIO directed (OCIO Directive 2005-007) a complete audit to verify that FY 2005 POA&M items were appropriately closed. Every program official was required to certify in writing that closed items met appropriate criteria for closure or re-

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

	open the weakness for action. While we saw a 25% increase in the number of new findings for FY 2005 Q3 and FY 2005 Q4, this increase is explained by the audits and self-assessments that occurred during this time period. In short, a 100% audit of 1.389 FY 2005 closed POA&M weaknesses (through Q3) did not conclude the same level of discrepancy as the 133 item sample in the POA&M report. Further, the draft POA&M report cites the September and November 2004 POA&M submission for a majority of its findings. That data is more than a year old and may not sufficiently characterize the FY 2005 POA&M program. Lastly, every POA&M weakness is prioritized within the system for which it is attributed. Point acknowledged by the OIG team. OCIO staff has discussed this point and commented to the report that a Departmental prioritization scheme is not required and administratively inappropriate. Each system is required to pursue appropriated funds through the relevant investment portfolio. Bureau managers may not reallocate those resources outside the portfolio based on Departmental priorities. Therefore, the most meaningful and effective prioritization is within each system. Additionally, this meets FISMA requirements and should be acknowledged as such.

IG's FISMA Section C Response	Question 4b
CIOs's FISMA Section B Response	No corresponding question(s)
Difference	Question 4b asks the IG to select from one of several response categories with respect to the degree to "When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)." The OIG selected the response category of "Rarely, for example, approximately 0-50% of the time" and in their comments on the FISMA response indicated that "Although DOI's POA&M process for IT security weaknesses includes the development, implementation, and management of POA&M for systems, DOI does not adequately manage the weaknesses adequately through its POA&M process." The OCIO has no basis in fact to suggest that program officials do not develop, implement, and manage POA&Ms for their systems when IT security weaknesses are identified. Therefore, the OCIO finds that the response category option of "Almost Always, for example, approximately 96-100% of the time" is a more appropriate

	characterization of compliance with respect to this question.
Discussion	The FISMA question specifically asks the question as to whether or not program officials (including CIOs) develop, implement, and manage POA&Ms for their systems when weaknesses are identified. The Department has demonstrated that there are POA&Ms for every system that is reported quarterly. Ideally, there would be a specific FISMA question, or questions, that inquire about specific quality characteristics of the POA&Ms and POA&M process. This particular FISMA question does not inquire about the quality or adequacy of either, and simply asks if program officials are managing weaknesses via their program or system POA&Ms. The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA. With respect to any questions regarding quality, raised in the comment section of the IG's FISMA report, the OIG relied on FY 2004 POA&Ms as the basis for their conclusions. The OIG's analysis did not take into consideration the substantial improvements to the FY 2005 POA&M process resulting from issuance of several OCIO Directives. In FY 2005, bureau CIOs were required to verify and validate completed actions on their POA&Ms and submit a signed certification statement attesting that they have done so with the submission of each of their quarterly POA&Ms. The OIG's report does not consider any FY 2005 progress and actually represents the state of the FY 2004 POA&M process. The characterization of Interior's POA&M process on the FISMA report should more appropriately reflect the effectiveness of the FY 2005 process. The OMB Memorandum 04-25 states the following with respect to the level of detail used to describe weaknesses in a POA&M: "Detailed descriptions of specific weaknesses are not necessary, but sufficient data is necessary to permit oversight and tracking. For example, to the maximum extent practicable agencies should use the types of descriptions commonly found in reports of the GAO and IG such as "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not been performed prior to system access," "physical access controls are insufficient," etc." Furthermore, OMB M-04-25 states that: "IGs are again asked to assess against minimum requirements

	whether the agency has developed, implemented, and is managing an agency-wide POA&M process (see Section C of the reporting template)." The IG's report should distinguish between when recommendations exceed the essential requirements of FISMA and OMB and be consistent in interpreting the adequacy or inadequacy of POA&M processes with respect to those "minimum requirements."

IG's Draft FISMA Section C Response	Question 4c
CIOs's Draft FISMA Section B Response	No corresponding question(s)
Difference	Question 4c asks the IG to select from one of several response categories with respect to the degree to which "Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress." The OIG selected the response category of "Sometimes, for example, approximately 51-70% of the time" and in their comments on the FISMA response indicated that "Although DOI program officials report to the CIO on a quarterly basis, we did not find any indications that contractors were reporting security weaknesses to program officials or bureau CIOs and that these security weaknesses were being reported by the program officials on the." This sentence was prematurely terminated but the CIO assumes that it was to conclude with the word POA&M. The OCIO has no basis to suggest that program officials. including contractors, do not report to the CIO on a regular basis (at least quarterly) on their remediation progress. Therefore, the OCIO finds that the response category option of "Almost Always, for example, approximately 96-100% of the time" is a more appropriate characterization of compliance with respect to this question. If the OIG's evaluation provides evidence to support their conclusion with respect to contractor reporting, then the OCIO believes that the response category of "Mostly, for example. approximately 81-95% of the time" would be appropriate. However. the OCIO is not aware of any specific details with respect to the absence of POA&Ms for contractor systems or any instances of non-reporting of POA&Ms to the CIO for such systems. The OCIO has provided copies of system POA&Ms and signed certification statements from relevant CIOs associated with the contractor systems to the OIG.

Discussion	We believe the OIG's comments need to be appropriately verified and validated. quantified in terms of the number of contractor systems for which such circumstances might be true, and compared to the total number of systems (government and contractor) in order to determine a reasonable approximation to use as the basis of the compliance estimation. For example. as the CIO is reporting that there are 10 contractor systems and 157 agency (government) systems. even assuming that the requirement was not met for any of the contractor systems but it was being met for all agency (government) systems. a more accurate characterization would be 157/167 or 94% compliance towards meeting this requirement.

IG's Draft FISMA Section C Response	Question 4d
CIOs's Draft FISMA Section B Response	No corresponding question(s)
Difference	Question 4d asks the IG to select from one of several response categories with respect to the degree to which the "CIO centrally tracks. maintains. and reviews POA&M activities on at least a quarterly basis." The OIG selected the response category of "Rarely, for example. approximately 0-50% of the time" and in their comments on the FISMA response indicated that "Although the CIO tracks and maintains POA&M activities on a quarterly basis we found little evidence that the POA&Ms are reviewed from the standpoint that weaknesses and related corrective actions were described and could be sufficiently acted upon and that reportedly corrected weaknesses were in fact corrected. There was also little indication that the DOI CIO sufficiently reviewed POA&M activities to ensure that all known IT security weaknesses were reported on the POA&M. This is demonstrated by the acceptance of risk that can be accomplished by DOI personnel that were not the appropriate officials for accepting such risks." The OCIO has no basis in fact to suggest that POA&M activities are not centrally tracked. maintained. or reviewed by CIOs on at least a quarterly basis. Therefore, the OCIO finds that the response category option of "Almost Always. for example. approximately 96-100% of the time" is a more appropriate characterization of compliance with respect to this question.

This level of compliance has been repeatedly demonstrated through Interior's quarterly POA&M reporting, tracking. and remediation progress and through the additional evidence provided to the OIG with respect to the signed POA&M certification statements by each |

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

	CIO as part of the last quarterly POA&M submission and reporting cycle.
Discussion	Assuming that an unauthorized individual was addressing the issue of risk acceptance on their own, without the concurrence of the Designated Approving Authority (DAA), the numbers of such occurrences are not quantified sufficient to suggest noncompliance. Compared to the thousands of weaknesses that are being tracked, managed, and reviewed, it is difficult to see how the OIG could conclude at this point that the number of any such instances could contribute to between 50% and 100% non-compliance with respect to this requirement. To the extent that the IG is aware of a number of such isolated incidents and has not identified such systemic issues on a larger and quantifiable scale it does not appear reasonable, for these occurrences to be used to extrapolate conclusion about noncompliance. The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA.

IG's Draft FISMA Section C Response	Question 4e
CIOs's Draft FISMA Section B Response	No corresponding question(s)
Difference	Question 4e asks the IG to select from one of several response categories with respect to the degree to which the "OIG findings are incorporated into the POA&M process." The OIG selected the response category of "Mostly, for example, approximately 81-95% of the time." The OCIO has no basis in fact to suggest that OIG findings are not being incorporated into POA&Ms. Therefore, the OCIO finds that the response category option of "Almost Always, for example, approximately 96-100% of the time" is a more appropriate characterization of compliance with respect to this question as there have been no known instances where OIG findings were not incorporated into the POA&M process.
Discussion	OIG "findings" are required to be always incorporated into the program- and system-level POA&Ms along with weaknesses identified from other sources. The CIO feels that the distinction would be that OIG "recommendations" are not always incorporated into the POA&M process as senior management does not always concur with such "recommendations" and has the discretion to consider whether or not such "recommendations" are required to be acted on or not. For the purpose of the FISMA report, the CIO

	requests that the OIG consider whether or not their response was based on the notion of incorporating "recommendations" vs. "findings", which might have contributed to a different perspective. The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA.

IG's Draft FISMA Section C Response	Question 4f
CIOs's Draft FISMA Section B Response	No corresponding question(s)
Difference	Question 4f asks the IG to select from one of several response categories with respect to the degree to which the "POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources." The OIG selected the response category of "Rarely, for example, approximately 0-50% of the time" and in their comments on the FISMA response indicated that "Currently bureaus prioritize weaknesses within system POA&Ms. However, we found little evidence that DOI overall prioritizes IT security weaknesses to ensure funding for this project..." The OCIO finds that the response category option of "Almost Always, for example, approximately 96-100% of the time" is a more appropriate characterization of compliance with respect to this question. The Department's POA&M process prioritizes IT security weaknesses consistent with OMB's requirements and within the constraints imposed by budgetary and capital planning and investment control (CPIC) processes.
Discussion	Interior's IT security program- and system-level POA&Ms include the appropriate level of detail and information required by the Office of Management and Budget (OMB) Memorandum 04-25. Prioritization of corrective actions is the responsibility of each Designated Approving Authority's (DAA's). Each DAA ensures that weaknesses are addressed in a timely manner and receives appropriate resources through their review and approval of their respective POA&Ms, which identify: • description of each weakness; • risk-level associated with each weakness; • specific corrective action milestones; • scheduled commitments to accomplish each milestone; and • resources (budgetary and staff) required to implement each

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 23 of 37

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

	corrective action.
	The DAA has the responsibility of making determinations regarding risk acceptance and the duration and conditions under which they will accept any residual risks.
	Lastly, every POA&M weakness is prioritized within the system for which it is attributed. Point acknowledged by the OIG team. OCIO staff has discussed this point and commented to the report that a Departmental prioritization scheme is not required and administratively inappropriate. Each system is required to pursue appropriated funds through the relevant investment portfolio. Bureau managers may not reallocate those resources outside the portfolio based on Departmental priorities. Therefore, the most meaningful and effective prioritization is within each system. Additionally, this meets FISMA requirements and should be acknowledged as such.
	The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA.

IG's Draft FISMA Section C Response	Question 5
CIOs's Draft FISMA Section B Response	No corresponding question(s)
Difference	Question 5 asks the IG to "assess the overall quality of the Department's certification and accreditation process." The OIG selected the response category of "Poor" without qualifying comments within the FISMA reporting template. The OCIO finds that the response category option of at least "Satisfactory" is a more appropriate characterization of compliance with respect to this question based on our analysis of the current state of the C&A process.
Discussion	In the OIG's Annual Evaluation report, the IG points to several factors contributing to their characterization of the Department's C&A process being rated as poor. The CIO maintains that the Department's Asset Valuation Guide (AVG) process to determine risk impact levels and security categorizations of systems for confidentiality, integrity, and availability equal or exceed any ratings based on the NIST FIPS Pub 199 and NIST SP 800-60 alone. The levels of concern expressed in appendix F of the Department's AVG guide used in determining potential impact ratings (e.g., Low,

Moderate, or High) for Confidentiality. Integrity, and Availability (CIA) are consistent with FIPS Pub 199. The AVG guide also identifies 15 sensitive information categories for Interior and the minimum expected impact ratings to be used for Interior's IT systems.

The Department's C&A, System Security Plan, Risk Assessment report, Security Test and Evaluation, and Contingency Planning guides substantially address the requirements of applicable NIST standards and guidelines.

The OCIO performed independent reviews of the quality of C&A packages and issued compliance reports back to each bureau identifying areas needing improvement. This process has resulted in many C&A packages being revised, resulting in significant improvement in the quality of those packages and 98% of Interior's systems are certified and accredited.

The OIG's report indicates that 8 of 17 systems reviewed had ST&E reports that were dated after they were accredited while the OCIO's records in Command Center indicate that approximately 31 of 171 C&A systems of record have ST&E reports dated after the date of the accreditation letter. This represents a potential concern with less than 20% of the C&A packages as opposed to the OIG's information indicating potential concerns with approximately 47% of the packages. These perspectives also don't identify whether or not the ST&Es were actually concluded prior to the DAA's decision to accredit their respective systems and whether or not those decisions were based on vulnerabilities and weaknesses identified in the ST&E. Consideration should be given to the actual dates within which the ST&Es were actually performed and the DAAs having had the benefit of those results as opposed to the date of the ST&E report documentation, which may have subsequently been revised based on feedback from independent reviews performed by the OCIO on the quality of those reports.

The IG's report does not contest the merits on which the DAA based their accreditation decision. which suggests that the certifications and accreditation are valid and based on each DAA's understanding and acceptance of any remaining residual risk to their systems.

With respect to the OIG's characterization of the POA&M process, the OIG relied on FY04 POA&Ms and did not benefit from a more recent study of the FY05 POA&Ms and associated process. The OCIO responded to these findings and recommendations in a separate response indicating that Interior's FY05 process has

| | substantially improved and that we had proactively taken measures to improve the process which already had addressed the IG's recommendations.

The OCIO recognizes the need to make some additional updates to C&A guidance in light of the significant number of new or revised standards and guidelines issued by NIST, which should be implemented in FY06 to implement FIPS Pub 200 and related SP 800-53 and 53a. Nonetheless, the CIO maintains that for FY05 the C&A process within Interior remains satisfactory. Beginning one year after the issuance of the FIPS Pub 200 by NIST, the CIO recognizes that existing System Security Plans and ST&E processes will be in jeopardy if these new requirements are not effectively implemented.

The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA. |
|---|---|

IG's Draft FISMA Section C Response	Question 6
CIOs's Draft FISMA Section B Response	Question 8
Difference	Question 6a asks "Is there an agency wide security configuration policy." The OIG selected the response of "Yes" and identified the relevant OCIO Directive. This question (both 6a and 6b) relates to agency policy and implementation of approved Security Technical Implementation Guides (STIGs). Each STIG provides specific security hardening and configuration instructions and parameters for various types of network resources and devices (e.g., operating systems. databases, routers, etc.) Question 6b asks the IG to "Approximate the extent of implementation of the security configuration policy on the systems running the software." The FISMA reporting template identifies 11 products for which the CIO and IG must select a response choice to indicate the degree to which systems have implemented approved STIGs. The CIO and IG differ in their response choices as there is a difference between our respective interpretations of what the FISMA questions are asking and the IG understands of Interior's policy.
Discussion	The OIG appears to be of the opinion that bureaus must implement the STIGs specified in Command Center (the Department's current IT security information dissemination portal) but acknowledges that bureaus frequently have their own STIGs which they implement.

	The CIO disagrees with the IG's interpretation as Interior's policy allows for bureaus to define, document, approve, and implement their own STIGs, which many have done. Bureaus are only required to implement the Department's STIGs available through Command Center whenever the bureau does not have their own approved STIG.
	The CIO believes that the OIG's criteria used to evaluate the degree to which Interior is compliant with this question exceed the essential requirements of FISMA. The OCIO also believes that the IG report does not reflect the same credit and degree of compliance with respect to bureau-level implementation of STIGs as the CIO's FISMA report reflects.

IG's Draft FISMA Section C Response	Question 7b
CIOs's Draft FISMA Section B Response	Question 9b
Difference	Question 7b asks does "The agency follow documented policies and procedures for external reporting to law enforcement." The OIG selected the response choice of "No" based on their observation that in 8 of 12 instances the OIG was not notified. Unlike many other response choices for other questions in the FISMA template, this is a binary answer and does not enable a more appropriate selection that would identify the relative frequency where such incidents are in fact reported to the IG or consideration of circumstances preventing full compliance with established external reporting procedures. The CIO feels that appropriate policies and procedures are in place and that there may be other mitigating circumstances that may have precluded adherence to these general procedures.
Discussion	Circumstances about why the 8 incidents were purportedly not reported via the IG were not sufficiently articulated. It is unclear what factors contributed to the lapse in notification for these specific incidents but it is clear that notification policies and procedures are in place and have successfully been used in other instances. The CIO acknowledges that Interior's policy requires notification of the OIG's Office of Investigations when IT security incidents are reported to external law enforcement. The CIO understands that the responsible OIG office was not well positioned for most of FY 2005 to receive, or respond to, such notifications. However, it should be recognized that Interior's bureaus and offices did engage other appropriate law enforcement officials to respond to incidents where appropriate.

IG's Draft FISMA Section C Response	Question 8
CIOs's FISMA Section B Response	Question 6
Difference	Question 8 asks "Has the agency ensured security training and awareness of all employees. including contractors and those employees with significant IT security responsibilities." The OIG selected the response choice of "Mostly, or approximately 81-95% of employees have sufficient training" which is inconsistent with the CIO's analysis.
Discussion	The OCIO's performance metrics with respect to annual awareness training and role-based training identifies the following relevant metrics in question 6 of the CIO's response:

a.	b.		c.	d.	
Total number of employees in FY05	Number of employees that received IT security awareness training in FY 05, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003)		Total number of employees with significant IT security responsibilities	Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)	
	Number	Percentage		Number	Percentage
84,159	82,848	98.44%	2611	1736	66.49%

The CIO is advocating that the progress in the areas of awareness and role-based training be equally weighted, which would result in the selection of "Almost Always, or approximately 96-100% of employees have sufficient training" based on the resulting weighted average of 97.48%. Additional credit should include recognition of the C&A training provided to the Secretary and Designated Approving Authorities (DAAs) by the CIO and CISO regarding the C&A process and each of their respective roles and responsibilities. Interior also has over 80 individuals who have achieved and are maintaining certification as a Certified Information Systems Security Professional (CISSP) from the International Information Systems Security Consortium, Inc., or (ISC)^2.

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name:

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2				
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of Systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Bureau of Indian Affairs	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized				1	0	1	1	100.0%	1	100.0%	1	100.0%
	Sub-total	0	0	0	1	0	1	1	100.0%	1	100.0%	1	100.0%
Bureau of Land Management	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		2			0	2	2	100.0%	2	100.0%	2	100.0%
	Sub-total	0	2	0	0	0	2	2	100.0%	2	100.0%	2	100.0%
Bureau of Reclamation	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		1			0	1	1	100.0%	1	100.0%	1	100.0%
	Sub-total	0	1	0	0	0	1	1	100.0%	1	100.0%	1	100.0%
Fish and Wildlife Service	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		1			0	1	1	100.0%	1	100.0%	0	0.0%
	Sub-total	0	1	0	0	0	1	1	100.0%	1	100.0%	0	0.0%
Minerals Management Service	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		1		1	0	2	2	100.0%	2	100.0%	2	100.0%
	Sub-total	0	1	0	1	0	2	2	100.0%	2	100.0%	2	100.0%
National Business Center	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		7		1	0	8	8	100.0%	7	87.5%	7	87.5%
	Sub-total	0	7	0	1	0	8	8	100.0%	7	87.5%	7	87.5%
National Parks Service	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		1			0	1	1	100.0%	0	0.0%	0	0.0%
	Sub-total	0	1	0	0	0	1	1	100.0%	0	0.0%	0	0.0%
Office of Special Trustee	High					0	0						
	Moderate					0	0						
	Low					0	0						
	Not Categorized		1			0	1	1	100.0%	1	100.0%	1	100.0%
	Sub-total	0	1	0	0	0	1	1	100.0%	1	100.0%	1	100.0%
						0	0						
Office of Surface Mining						0	0						
U.S. Geological Survey						0	0						
						0	0						
Other OIG Reviews:						0	0						
Financial Audits						0	37						
Penetration Testing						0	11						
SCADA-NCIIS						0	4						
POAM						0	20						
Wireless						0	5						
Agency Totals	**High**	0	0	0	0	0	0	0		0		0	
	Moderate	0	0	0	0	0	0	0		0		0	
	Low	0	0	0	0	0	0	0		0		0	
	Not Categorized	0	14	0	3	0	94	17		15		14	
	Total	0	14	0	3	0	94	17		15		14	

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Frequently, for example, approximately 71-80% of the time

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

DoI's FY 2005 FISMA Report
Page 29 of 37

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.
	
	Response Categories:
	  - Approximately 0-50% complete
	  - Approximately 51-70% complete
	  - Approximately 71-80% complete
	  - Approximately 81-95% complete
	  - Approximately 96-100% complete
		- Approximately 81-95% complete

3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes

Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

  - Rarely, for example, approximately 0-50% of the time
  - Sometimes, for example, approximately 51-70% of the time
  - Frequently, for example, approximately 71-80% of the time
  - Mostly, for example, approximately 81-95% of the time
  - Almost Always, for example, approximately 96-100% of the time

4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Sometimes, for example, approximately 51-70% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Rarely, for example, approximately 0-50% of the time"
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Sometimes, for example, approximately 51-70% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Rarely, for example, approximately 0-50% of the time"
4.e.	OIG findings are incorporated into the POA&M process.	- Mostly, for example, approximately 81-95% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Rarely, for example, approximately 0-50% of the time"

Comments: 4.a.Response: Sometimes – 51-70%. However, we did not determine the amount of unreported IT security weaknesses that were not included in the POA&Ms. 4.b. Response: Rarely 0-50%. Although DOI's POA&M process for IT security weaknesses includes the development, implementation, and management of POA&M for systems, DOI does not manage the weaknesses adequately through its POA&M process. This is demonstrated by the number of weaknesses we identified that were reported as corrected, but were not corrected, that weakness descriptions and related corrective actions were not sufficient to ensure that the weakness was understood by management or that the related corrective actions would correct the weakness. 4.c. Response: Sometimes – 51-70%. Although DOI program officials report to the CIO on a quarterly basis, we did not find any indications that contractors were reporting security weaknesses to program officials bureau CIOs and that these security weaknesses were being reported by the program officials on the 4.d. Response: Rarely 0-50%. Although the CIO tracks and maintains POA&M activities on a quarterly basis we found little evidence that the POA&Ms are reviewed from the standpoint that weaknesses and related corrective actions were described
and could be sufficiently acted upon and that reportedly corrected weaknesses were in fact corrected. There was also little indication that the DOI CIO sufficiently reviewed POA&M activities to ensure that all known
IT security weaknesses were reported on the POA&M. This is demonstrated by the acceptance of risk that can be accomplished by DOI personnel that were not the appropriate officials for accepting such risks.
4.e. Response: Mostly 80-95%. 4.f. Response: Rarely 0-50%. Currently bureaus prioritize weaknesses within system POA&Ms. However, we found little evidence that DOI overall prioritizes IT security weaknesses to ensure
significant IT security weaknesses are addressed in a timely manner and receive appropriate resources. The only exception is that DOI did prioritize the certification and accreditation of IT systems and obtained the necessary
funding for this project. Nonetheless, not all of DOI's systems have been certified and accredited and not all significant deficiencies within these accredited systems have been corrected. Additional Comments: In response
to the briefing Office of Audits provided to the DOI IT Management Council in April 2005, the DOI CIO issued a Directive requiring bureaus and offices to review previously reported corrected weaknesses and certify whether
those weaknesses were in fact corrected and if not corrected report the weakness. We have not verified whether this Directive has been effectively followed by the bureaus and offices

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans .

	Assess the overall quality of the Department's certification and accreditation process.
	
	Response Categories:
	  - Excellent
	  - Good
	  - Satisfactory
	  - Poor
	  - Failing
		- Poor

Comments:

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name:

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes

Comments: OCIO Directive 2004-007, March 05, 2004, Standardized System Security Configuration

6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	Addressed in agencywide policy? Yes, No, or N/A.	Do any agency systems run this software? Yes or No.	Approximate the extent of implementation of the security configuration policy on the systems running the software. Response choices include: - **Rarely, or, on approximately 0-50% of the systems running this software** - **Sometimes, or on approximately 51-70% of the systems running this software** - **Frequently, or on approximately 71-80% of the systems running this software** - **Mostly, or on approximately 81-95% of the systems running this software** - **Almost Always, or on approximately 96-100% of the systems running this software**
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Solaris	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
HP-UX	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Linux	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Oracle	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Other. Specify:	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software

Comments: Other: AIX, Apache Web Servers, Remote Access Servers

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	No
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: 7.b. We identified Eight (8) instances of non-compliance from November 2004 through August 2005. Training was provided.

Question 8

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

I. Senior Agency Official for Privacy Responsibilities

1.	Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)? Yes or No.	Yes
2.	Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19? Yes or No.	Yes
3.	Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information? Yes or No.	Yes

Comments: *Concerning Question #3: The DOI CIO has delegated the "Reviewing Official" function for signing PIAs to the CIO or equivalent of the bureaus/offices responsible for the system. The DOI PIA includes an analysis of privacy risks when new technology is being considered.*

II. Procedures and Practices

1.	Does your agency have a training program to ensure that all agency personnel and contractors with access to Federal data are generally familiar with information privacy laws, regulations and policies and understand the ramifications of inappropriate access and disclosure? Yes or No.	Yes
2.	Does your agency have a program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities)? Yes or No.	Yes
3.	Section 3, Appendix 1 of OMB Circular A-130 requires agencies conduct -- and be prepared to report to the Director, OMB on the results of -- reviews of activities mandated by the Privacy Act. In the chart below, please indicate by component (e.g., bureau, agency) which of the following reviews were conducted in the last fiscal year. *(Note: Except for Matching Programs, when FY05 was the "off-year" a " N/A " was reported. The FY the review will be completed is listed next to that)*	

Bureau	Section M Contracts	Records Practices	Routine Uses	Exemptions	Matching Programs	Training	Violations	Systems of Records	
Bureau of Indian Affairs	N/A 2006	Yes	NA 2006	Yes	N/A	Yes	N/A 2006	Yes	
Bureau of Land Management	Yes	Yes	Yes	Yes	N/A	Yes	N/A	N/A 2006	
Bureau of Reclamation	Yes	Yes	N/A 2006	N/A 2006	N/A	Yes	N/A	N/A 2006	
Fish and Wildlife	Yes	Yes	Yes	Yes	N/A	Yes	Yes	Yes	
Minerals Management Service	N/A 2006	Yes	N/A 2006	Yes	N/A	N/A 2006	Yes	N/A 2006	
National Park Svc	NA 2006	N/A 2006	N/A 2006	Yes	N/A	N/A 2006	Yes	N/A 2006	
Ofc of Inspector General	N/A 2006	N/A 2006	N/A 2006	Yes	N/A	N/A 2006	N/A 2006	N/A 2006	
Ofc of the Secretary	N/A 2006	N/A 2006	N/A 2008	N/A 2008	N/A	N/A 2006	N/A 2006	N/A 2006	
Ofc of Surface Mining	N/A 2006	Yes	N/A 2006	N/A 2006	N/A	N/A 2006	N/A 2006	Yes	
Solicitor	N/A 2006	Yes	N/A 2006	N/A 2006	N/A	N/A 2006	N/A 2006	N/A 2006	
U.S. Geological Svc.	Yes	N/A 2006	N/A 2006	Yes	N/A	Yes	Yes	N/A 2006	

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

4.		Section 208 of the E-Government Act requires that agencies (a.) conduct Privacy Impact Assessments under appropriate circumstances, (b.) post web privacy policies on their websites, and (c.) ensure machine-readability of web privacy policies.			
	a.	Does you agency have a written process or policy for:			
		(i.)	determining whether a PIA is needed? Yes/No		Yes
		(ii.)	conducting a PIA? Yes/No		Yes
		(iii.)	evaluating changes in business process or technology that the PIA indicates may be required? Yes/No		Yes
		(iv.)	ensuring that systems owners and privacy and IT experts participate in conducting the PIA? Yes/No		Yes
		(v.)	making PIAs available to the public in the required circumstances? Yes/No		Yes
		(vi.)	making PIAs available in other than required circumstances? Yes/No *(DOI requires that PIAs be completed for IT Security Certifications)*		Yes
	b.	Does your agency have a written process for determining continued compliance with stated web privacy policies? Yes/No			Yes
	c.	Do your public-facing agency web sites have machine-readable privacy policies (i.e., are your web privacy policies P3P-enabled or automatically readable using some other tool)? Yes/No *(Interior Main webpage compliant - Bureaus will implement by 12/31/05)*			No
		(i.)	if not, provide date for compliance:		12/31/2005

Section D: Senior Agency Official for Privacy. W. Hord Tipton, Chief Information Officer, Department of the Interior

Agency Name:Department of the Interior

II. Procedures and Practices, Continued.

5. By bureau, Identify the number of information systems containing Federally-owned Information in an identifiable form. For the applicable systems, on how many have you conducted a Privacy Impact Assessment and published a Systems of Records Notice?

| | a. | | | b. | | | | | | c. | | | | | |
| | FY 05 Systems that contain Federally-owned Information in an identifiable form | | | FY 05 Privacy Impact Assessments: total number requiring a Privacy Impact Assessment In FY 05 (systems that are new or have been substantially altered) | | | FY 05 Privacy Impact Assessments: number that have a completed Privacy Impact Assessment within FY 05 | | | FY 05 Systems of Records Notices: By bureau: number of systems from which Federally-owned Information is retrieved by name or unique identifier | | | FY 05 Systems of Records Notices: number of systems for which one or more Systems of Records Notice/s have been published in the Federal register | | |
Bureau Name	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems	Agency Systems	Contractor Systems	Total number of Systems
Bureau of Indian Affairs	20		20	20		20	4		4	24		24	24		24
Bureau of Land Management	0	0	0	0		0	0		0	22		22	22		22
Bureau of Reclamation	0		0	0		0	0		0	24		24	24		24
Fish and Wildlife Svc	24		24	16		16	8		8	21		21	18		18
Minerals Management Svc	2	0	2	2		2	2		2	1		1	1		1
National Parks Svc	3		3	3		3	2		2	6		6	6		6
Inspector General	4	1	5	4	1	5	2		2	4	1	5	1		1
Office of the Secy	2	1	3	2		2	2		2	19	1	20	19	1	20
Office of Surface Mining	1		1	1		1	1		1	1		1	1		1
Solicitor	6		6	6		6	5		5	6		6	5		5
USGS	12		12	12		12	12		12	10	1	11	10	1	11
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
			0			0			0			0			0
Agency Totals			76			67			38			141			133

5.d.   Contact Information for preparer of Question 5: Marilyn Legnini, 202-219-0868, Marilyn_Legnini@ios.doi.gov

Question 6

OMB policy (Memorandum 03-22) prohibits agencies from using persistent tracking technology on web sites except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).

Subject to Protective Order
Regarding I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

REDACTED PUBLIC VERSION
DoI's FY 2005 FISMA Report
Page 35 of 37

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

6.a.	Does your agency use persistent tracking technology on any web site? Yes/No	Yes
6.b.	Does your agency annually review the use of persistent tracking? Yes/No	Yes
6.c.	Can your agency demonstrate through documentation the continued justification for and approval to use the persistent technology? Yes/No	Yes
6.d.	Can your agency provide the notice language used or cite to the web privacy policy informing visitors about the tracking? Yes or No.	Yes
III. Internal Oversight		
1.	Does your agency have current documentation demonstrating review of compliance with information privacy laws, regulations and policies? Yes or No *(Note: DOI is continuing to develop standard processesl for FY2006)*	Yes
(i.)	If so, provide the date the documentation was created:	10/18/2002
2.	Can your agency provide documentation demonstrating corrective action planned, in progress or completed to remedy identified compliance deficiencies? Yes or No. *(Note: DOI is developing additional oversight tools for 2006)*	Yes
(i.)	If so, provide the date the documentation was created:	3/25/2005
3.	Does your agency use technologies that allow for continuous auditing of compliance with stated privacy policies and practices? Yes or No. *(Note: DOI is exploring options for a Depl standard tracking system)*	No
(i.)	If so, provide the date the documentation was created:	MM/DD/YYYY
4.	Does your agency coordinate with the agency Office of Inspector General on privacy program oversight by providing to OIG the following materials:	
(a.)	compilation of the agency's privacy and data protection policies and procedures? Yes/No	Yes
(b.)	summary of the agency's use of information in identifiable form? Yes/No	Yes
(c.)	verification of intent to comply with agency policies and procedures? Yes/No	Yes
5.	Does your agency submit an annual report to Congress (OMB) detailing your privacy activities, including activities under the Privacy Act and any violations that have occurred? Yes or No.	Yes
(i.)	If so, when was this report submitted to OMB for clearance?	12/6/2004

Section D - Senior Agency Official for Privacy W. Hord Tipton, Chief Information Officer, Department of the Interior

Agency Name: Department of the Interior

IV. Contact Information

	Name	Phone Number	E-mail Address
Agency Head	Gale Norton	202-208-7351	Gale_Norton@ios.do
Chief Information Officer	W. Hord Tipton	202-208-6194	Hord_Tipton@ios.do
Agency Inspector General	Earl Devaney	202-208-5745	Earl_Devaney@oig.c
Chief Information Security Officer	Larry Ruffin (Acting)	202-208-5419	Lawrence_Ruffin@ic
Senior Agency Official for Privacy	W. Hord Tipton	202-208-6194	Hord_Tipton@ios.do
Chief Privacy Officer			
Privacy Advocate			
Departmental Privacy Officer	Marilyn Legnini	202-219-0868	Marilyn_Legnini@ios
Reviewing Official for PIA's	Bureau CIOs		

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, DC 20240

OCT - 6 2005

2005 OCT -6 4:25

Memorandum

To: Secretary

From: Earl E. Devaney
            Inspector General

Subject: Annual Evaluation of the Information Security Program of the Department
            of the Interior (Report No. NSM-EV-MOI-0013-2005)

The attached report presents the results of our annual evaluation of the U.S.
Department of the Interior's (DOI) Information Technology (IT) security program, as
required by the Federal Information Security Management Act (FISMA).

Again this year, we concluded that the Department continues to make progress to
improve the security over its information systems. The report highlights a number of
positive steps including the Department's improvements to the Security Training and
Awareness program, and a significant effort to implement the Enterprise Services
Network to bolster security efforts.

Based on the findings of our evaluation in 2005, however, we believe that DOI is not
in compliance with the requirements of FISMA.

Our testing and evaluation of DOI's IT Security program for Fiscal Year 2005
indicates that DOI has weaknesses in three critical areas: network security, Plans of
Actions and Milestones (POA&M), and Certification & Accreditation (C&A)

Our penetration testing program revealed a network infrastructure that was vulnerable
to unauthorized access and allowed us to compromise some of DOI's most sensitive
information. Our review of the DOI POA&M process shows that DOI cannot be assured
that the POA&M, in its current state, can be used as the authoritative tool to manage IT
security weaknesses. We have recommended that the Department report the POA&M
process as a material weakness in 2005 under the Federal Manager's Financial Integrity
Act. We have rated the Department's C&A program as poor based on a number of
factors, including failure to apply Federal Information Processing Standard 199, the
previously mentioned problems with POA&Ms, and completion of Security Test and
Evaluation work subsequent to C&A for some systems.

If you have any questions about this report, please call me at (202) 208-5745.

Attachment

Table of Contents

Executive Summary

This report presents the results of our evaluation of the U.S. Department of the Interior's (DOI) information security program for Fiscal Year (FY) 2005. The objective of our evaluation was to (1) determine whether DOI's information security program satisfied the requirements of the Federal Information Security Management Act of 2002 (FISMA)[1] and (2) obtain information necessary to respond to Office of Management and Budget (OMB) questions[2] about DOI's security program.

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

Additionally, problems in DOI's overall Plan of Actions and Milestones program, which is designed to manage and prioritize remediation activities, indicate that DOI management cannot be assured that IT security risk is properly identified, understood, prioritized, and mitigated. As such, DOI should report its Plan of Actions and Milestones program as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the 2005 Performance and Accountability Report.

Our penetration testing program revealed poor network and application security, inadequate network segmentation, and poor security configurations. These weak security controls make DOI vulnerable to unauthorized access from internal and external threats.

Perhaps most troubling has been the lack of an effective agency-wide strategy to implement and oversee the various DOI-issued polices and procedures. Fieldwork continues to demonstrate that bureaus do not adhere to DOI policy – and in many cases are unaware of its existence – and self report IT security metrics with little validation. While DOI has taken a number of positive steps to address the various deficiencies that we have uncovered in the past, unfortunately, our fieldwork and evaluation activities reveal significant problems continue to exist with the overall DOI IT security program.

---

[1] 44 U.S.C. Chapter 35.

[2] Memorandum M-05-15, FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, June 13, 2005

Background

Congress enacted FISMA to provide a comprehensive framework to secure the federal government's information and IT resources. FISMA requires federal agencies to implement security programs that protect information systems and data from unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, FISMA requires, overall, that security programs equip federal agencies with mechanisms to accomplish the following:

- Assess risks and implement policies and procedures to reduce risks.
- Test and evaluate security controls.
- Plan for continuity of operations.
- Maintain subordinate plans for providing information security.
- Plan for security throughout the life cycle of systems.
- Plan corrective actions.
- Train employees and contractors.
- Detect, report, and respond to security incidents.

Prior to the enactment of FISMA, DOI lacked a formal IT Security program. There was inadequate funding, little management focus, and certainly no accountability. The lack of agency-wide policy and procedures only compounded the confusion within the bureaus and offices making implementation problematic. The IT management within the bureaus was nonresponsive to various efforts made by DOI's Office of the Chief Information Officer (OCIO) to improve DOI's overall IT Security program.

Over time, the OCIO has created a large assemblage of policies and procedures for IT operations and security that complement the government standards established by OMB and the National Institute of Standards and Technology (NIST). Prior to FISMA, our work found such a lack of policies and guidance that we simply pointed to inadequate IT security as our major finding.

Since the enactment of FISMA, DOI's IT Security program has seen increased management awareness, involvement, focus, and funding. IT security staffing has also increased and adequate training has been made available to the general workforce. During FY 2004 and 2005, DOI essentially established a body of policy and guidance and invested in various security technologies – at an estimated cost of $100 million – needed to create a control environment that allows testing of the networks, systems, and programs comprising DOI's IT assets. This has allowed our evaluation efforts to evolve from an essentially general controls-based auditing approach to one where technical experts conduct valid and real-world tests on the security of DOI's networks and computer infrastructure.

While our comprehensive FISMA evaluation points out significant weaknesses, we note that DOI has taken several positive steps to improve its overall security, including the following:

- Implementation of the DOI-wide Enterprise Services Network to provide a more secure computing and networking environment.

- Enhancing the DOI vulnerability scanning program beyond just the SANS Top 20[3] list of vulnerabilities.

- Implementation of Active Directory and the use of group policy for enforcing Microsoft-based security configurations.

- Significant improvements in content and usability of the DOI End User IT Security Training and Awareness Program.

- Completing its E-Authentication risk assessments.

---

[3] See http://www.sans.org/top20/ for the latest expert consensus on the top twenty security vulnerabilities facing Windows and UNIX based systems.

REDACTED PUBLIC VERSION
Annual Evaluation of the
Information Security Program of DoI
Page 5 of 45

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

Evaluation Methodology

We performed our evaluation, as applicable, in accordance with Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency. We focused on validating the implementation of various DOI policies and procedures within the bureaus and answering OMB's questions for Inspectors General for the FY 2005 FISMA report.

Unfortunately, in implementing this approach, we experienced a number of difficulties carrying out our FISMA evaluations this year. Coordinating our testing activities with DOI was hindered by the OCIO's lack of initial cooperation. This required us to modify various testing techniques, particularly those related to our technical evaluations. In one instance, our team was not allowed to connect to the Mineral Management Service (MMS) network based on instructions MMS received from the OCIO. Additionally, OCIO provided information late, and the information was often incomplete and unreadable. These delays caused us to exclude two bureaus – Office of Surface Mining and the U.S. Geological Survey – from our annual evaluation in order to meet OMB's reporting deadline.

To accomplish our evaluation we did the following:

- Conducted FISMA-specific evaluations on 17 systems, including three systems operated by contractors (see Appendix I), according to instructions from OMB.

- Conducted penetration testing on all of DOI's major networks to identify, document, and attempt exploitation of vulnerabilities that could be used to gain access to DOI systems. as well as evaluated DOI's incident response capabilities.

- Conducted fieldwork to assess the effectiveness of management, operational, and technical controls in use at DOI's National Critical Infrastructure Information Systems.

- Integrated our FISMA evaluation activities with the ongoing financial audit.

- Reviewed and evaluated DOI's Plan of Actions and Milestones Program.

- Reviewed and evaluated relevant IT security documentation related to DOI's Certification and Accreditation program.

We did not evaluate security controls on DOI's national security information systems because they are subject to review by the Central Intelligence Agency.

Specifically, we conducted our technical compliance testing throughout the year to test the effectiveness of deployed controls across networks, applications, servers, and workstations. We also carried out field inspections and general control reviews in the following seven FISMA compliance areas:

1. System inventory, including contractor-operated systems.

2. Certification and Accreditation, including system security planning, interconnections, and contingency planning.

3. Plan of Actions and Milestones.

4. Computer security incident response.

5. Security assessments.

6. Security configurations.

7. Security training and awareness.

This year we also established a quarterly FISMA update reporting process. We initiated this process to provide DOI's management with an integrated view of our findings through various investigations, audits, and IT-related evaluations regarding the state of IT security on a quarterly basis.

Evaluation Results

System Inventory[4]

FISMA requires that agencies have an inventory of their major IT systems, whether operated by the agency or third parties, such as contractors, who are working on behalf of the agency. The inventory must be maintained and updated at least annually and system interfaces must be identified.

DOI's official inventory system is the Departmental Enterprise Architecture Repository (DEAR). DOI's bureaus use a localized version known as the Bureau Enterprise Architecture Repository (BEAR) to manage their system inventories.

We found that DOI does have an inventory system in place but still relies on manual efforts to reconcile various system counts, and uses a separate inventory system for its security program. After detailed discussions with DOI, we generally agree with DOI on the number of systems contained in the inventory. While we did not observe any major information systems missing from DEAR, we do not feel that DOI has an efficient process in place and are concerned by the various different inventories used to report system counts. We will be carrying out a more through review next year.

Our findings are noted below:

- National Security Systems are neither identified in DEAR nor are there place holders for shell records.

- Bureaus had significantly more information available on their system components than what was reported in DEAR.

- Individuals with significant security responsibilities were not aware of DEAR or BEAR.

- For IT Security reporting purposes, DOI maintains a separate inventory system that is not integrated with DEAR, raising additional concerns for all subsystems being fully identified and their interfaces documented.

- Using multiple inventories for reporting makes it difficult to maintain an accurate system count.

DOI is working on linking lesser systems to their respective "parent" system, known as an enclave. The OCIO is currently in the process of matching Certification and

---

[4] (OMB Questions C1a, b, c and 3b, c, d, e).

Accreditation systems, which are maintained in a separate inventory, to the member DEAR system. Also, enclave to subsystem reconciliation is not yet complete and relies on manual processes. As these manual reconciliation efforts go on, discrepancies in the inventory should be reduced, but for the time being, DOI cannot be assured of a completely accurate system inventory.

Additionally, we inspected the security plans to verify that systems and General Support Systems/Enclave subsystems were properly included. Upon inspection, we noted the following discrepancies:

- The National Business Center (NBC) Denver Data Center mainframe is detailed separately in the Denver Data Center Enclave System Security Plan documentation. However, it is not listed in the system inventory, as are the other member systems documented in the system security plan and the system inventory.

- The NBC Reston Local Area Network (LAN) lists the Travel Management System, Consolidated Financial System (CFS), and Interior Department Electronic Acquisition System (IDEAS) as member systems in the system inventory. However, they are not detailed separately in the Reston LAN system security plan documentation.

We also note that differing definitions are sometimes used to determine what exactly constitutes a system, a subsystem, or an enclave. While there is guidance from DOI to define and track systems, DOI should enforce a consistent definition and methodology[5].

Contractor Operations and Oversight[6]

FISMA, OMB, and DOI policy requires contractor-operated systems to meet the same minimum security requirements as systems operated by the federal government. On August 18, 2004, DOI issued a policy document concerning IT security for its acquisitions and contracts[7]. This policy establishes very clear requirements and guidelines to assist business managers in ensuring that adequate IT security requirements are part of the contracting process. None of the personnel involved with the three contractor-operated systems – the Bureau of Indian Affairs, the NBC/the Office of the Secretary, and the MMS – we reviewed were aware of this policy. DOI staff – including contracting officers, contracting officer's technical representatives, security liaisons, and the contractors' staff – had never seen the policy.

---

[5] The policies and procedures for populating the system inventory are widely accessible via the project's Web site, *http://www.doi.gov/ocio/architecture/index.html.* Guidelines are in place to eliminate duplication of records and define what constitutes a system that should be tracked in the database.

[6] OMB Question C3a.

[7] DOI Memorandum "Information Technology Security Requirements for Acquisition," August 18, 2004.

Of the three contracts we reviewed, none included DOI's requirements or were reviewed for compliance with DOI's guidance. Additionally, none of the bureaus had reported back to DOI on their contracts' compliance with DOI's guidance, as prescribed in the policy document.

We found that the bureaus, acting on their own, have ensured that oversight activities are carried out and that the systems have gone through Certification and Accreditation. However, each organization handles contract oversight differently and with differing levels of rigor. We felt that BIA's oversight process was very effective, even though it was not aware of DOI's policy and had not formalized it within the contract. MMS, however, was not allowed to fully inspect a subcontractor's production environment or to test it technically due to contractual issues, making the overall value of its oversight process questionable. Our testing efforts of the same MMS subcontractor were also hindered by the lack of appropriate language in the contract. Thus, we were prevented from physically inspecting the servers hosting the MMS data or carrying out any technical testing. Ironically, at essentially the same time period as our inspection attempts, hackers compromised this subcontractor-operated system. The vulnerability leading to the compromise could very well have been discovered if MMS or the OIG had been allowed to carry out testing. We later learned that this same application had been hacked up to four times previously.

While oversight is occurring at the bureau level, DOI's management cannot be assured of its effectiveness or compliance with DOI's own policy for IT Security in acquisitions. Even when a bureau concurs with an audit recommendation pertaining to contracting, DOI cannot be assured that it has been carried out. For example, in a follow up to an IT security audit in FY 2004, we notified DOI on August 29, 2005[8], that one of its bureaus had failed to carry out modifying all IT contracts to require position sensitivity designation and the appropriate background investigation. These were actions that the bureau director had advised would be corrected by September 30, 2004.

Plan of Actions and Milestones Program[9]

FISMA requires federal executive branch agencies to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices. OMB designed the Plan of Actions and Milestones to meet this requirement.[10] The guidance requires

---

[8] OIG Memorandum "Status Report on One Recommendation From the Audit Report Titled 'Improvements Needed in Managing Information Technology System Security, National Park Service' (Assignment No. A-ST-NPS-0005-2005)," August 29, 2005.
[9] OMB Question C4.
[10] OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plan of Actions and Milestones," issued October 17, 2001. This guidance was updated by OMB Memorandum M-03-19,

that Plan of Actions and Milestones (1) include all security weaknesses found during any review done by, for, or on behalf of the organization; (2) prioritize remediation activities; (3) be tied to the organization's budget submission through the unique project identifier of a system; and (4) be used as the authoritative project management tool for tracking and correcting security weaknesses. DOI's bureaus are required to prepare Plan of Actions and Milestones for each of their systems and programs where security weaknesses have been identified. The OCIO, using the bureaus' data, prepares a DOI-wide Plan of Actions and Milestones that is submitted to OMB. It is also used to report progress on remediation efforts to correct security weaknesses to OMB and the Congress. OCIO has stated that the Plan of Actions and Milestones is DOI's authoritative tool for managing IT security weaknesses.

We have been assessing DOI's Plan of Actions and Milestones process since 2002 and have noted that although DOI implemented a process, challenges remain in ensuring its effectiveness and accuracy. Weaknesses with the process indicate that the Plan of Actions and Milestones Program, in its present state, cannot be viewed as an agency process that (1) incorporates all known IT security weaknesses, (2) has program officials who are held accountable for managing their processes, (3) prioritizes weaknesses, and (4) has an OCIO that exercises adequate oversight and review of the process.

Our work in FY 2005 was our most comprehensive effort to date. We examined a sample of 344 items and tested 133 for compliance, which revealed systemic problems with the Plan of Actions and Milestones process[11]. Given our findings, DOI should report its Plan of Actions and Milestones program as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the 2005 Performance and Accountability Report. Summaries of our major findings from the evaluation are noted below:

- Sixty-four items out of 133, or roughly 48 percent, that had been reported as corrected were in fact not corrected.

- Not all known weaknesses were included in DOI's Plan of Actions and Milestones.

- Bureaus used differing, and sometimes arbitrary, definitions to determine what would be included and excluded from the Plan of Actions and Milestones.

"Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting," issued on August 6, 2003.
[11] Report: A-EV-MOA-0001-2005 "Evaluation Report on the Department of the Interior's Process to Manage Information Technology Security Weaknesses," September 2005.

- Descriptions of weaknesses and the required actions to correct them were not adequate.

- The OCIO has not instituted adequate quality assurance and verification measures to ensure the accuracy of its Plan of Actions and Milestones.

- Responsible officials are not held accountable for the accuracy of the information and for correcting the weaknesses.

- There is no effective DOI-wide process to ensure that weaknesses are prioritized based on the risk to DOI.

- There is insufficient documentation or justification for accepting risk as a means to close out a Plan of Actions and Milestones item.

We note that the OCIO has issued policy and instructions to significantly improve DOI's Plan of Actions and Milestones process and address the OIG's findings[12]. We observed fast responsiveness in the field to carry out DOI's new guidance. We will validate the implementation, accuracy, and completeness of these new guidelines in FY 2006.

Certification and Accreditation Program[13]

In this year's FISMA reporting guidance, OMB has asked the OIG to provide a "qualitative assessment" of the agency's Certification and Accreditation process. The assessment required us to determine adherence to existing policy, guidance, and standards to determine if DOI is using NIST Special Publication 800-37[14] and other relevant NIST publications for Certification and Accreditation work initiated after May 2004. This includes use of Federal Information Processing Standards (FIPS) 199[15] to designate impact levels to the confidentiality, integrity, and availability of a system.

In our FY 2004 FISMA report, the OIG gave DOI a satisfactory rating on its assessment of the DOI Certification and Accreditation program in part because DOI had initiated a quality assurance process to carry out detailed evaluations of the relevant

---

[12] OCIO Directive 2005-007. FY 2005 Plan of Actions and Milestones Process Verification. May 3, 2005, and OCIO Memorandum "Implementing OCIO Directive 2005-007 for 4th Quarter Plan of Actions and Milestones (POA&M) and 4th Quarter Federal Information Security Act Performance Measures, August 18. 2005.

[13] OMB Questions C2 and C5.

[14] Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004.

[15] Standards for Security Categorization of Federal Information and Information Systems, February 2004.

REDACTED PUBLIC VERSION
Annual Evaluation of the
Information Security Program of DoI
Page 12 of 45

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

documents. Since DOI's implementation of the Certification and Accreditation quality assurance process in FY 2004, the OIG has had a chance to review the process as well[16].

Overall, based on this year's evaluation work, we have rated the Department's Certification and Accreditation program as **POOR**.

To carry out this assessment, we reviewed Certification and Accreditation documentation for the 17 systems that made up our FISMA subset analysis, four National Critical Infrastructure Information Systems, selected systems reviewed by the OCIO in its quality assurance reviews, and relevant DOI Certification and Accreditation documents. Overall, we found that DOI has a large body of procedures and documentation in place to assist system owners in accomplishing their Certification and Accreditation activities. While these procedures helped DOI initially achieve Certification and Accreditation on their systems, the overall process is poor because of the following:

- Very little or no work has been done on meeting FIPS 199 requirements.

- DOI Certification and Accreditation process is inconsistent with the NIST framework.

- DOI documentation has not been updated sufficiently.

- DOI "how-to" guides are out of date.

- Weaknesses in the Plan of Actions and Milestones process directly impact the DOI Certification and Accreditation program.

- Some systems Security Test and Evaluation reports were dated after the systems were signed off for full Accreditation.

- Employees, especially approving officials, were not trained adequately.

We observed that bureaus, such as the Bureau of Land Management, that had strong, dedicated project managers assigned to oversee the various complexities of the processes, had much better control over maintaining their systems Certification and Accreditation.

---

[16] A large number of DOI's systems have been Certified and Accredited and deemed by DOI to have effective controls in place to provide adequate security. In the OIG annual FY04 FISMA report, the OIG gave DOI a satisfactory rating on its assessment of the DOI C&A program in part because DOI had initialized a Quality Assurance process to carry out detailed evaluations of the relevant C&A documents. The OIG was not able to review the process in the FY 2004 reporting period as DOI had just undertaken this effort.

FIPS 199 Findings

For FY 2005, OMB asked agency chief information officers and Inspectors General to determine the extent to which agencies are in compliance with FIPS 199. As OMB explains in this year's reporting instructions:

> "FISMA tasked NIST to develop a standard to categorize all information and information systems based upon the need to provide appropriate levels of information security according to a range of risk levels. FIPS Publication 199, "Federal Information Processing Standard 199: Standards for Security Categorization of Federal Information and Information Systems" (February 2004) defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). These impact levels are: low, moderate, and high. All agencies must categorize their information and information systems using one of these three categories in order to determine which security controls in NIST Special Publication 800-53 should be implemented.[17]"

By understanding, evaluating, and assigning the appropriate impact levels to a given system and its information, DOI can assign the appropriate security safeguards. In our fieldwork, we discovered that 15 of the 17 systems lacked a FIPS 199 impact designation[18], even though this has been a federal standard and requirement since February 2004. Most of these systems were accredited after May 2004. Through our reviews of Certification and Accreditation documentation and interviews with security staff, we determined that very little or no work has been carried out to meet FIPS 199 standards and that bureaus are looking for guidance from DOI. For example, the BOR Wide Area Network and the NBC/Office of the Secretary Drug Testing system had been recertified and accredited, respectively, in FY 2005, but still lacked FIPS 199 categorizations.

Overall, FIPS 199 forms the basis for an effective risk assessment and management program. Failure to implement or achieve compliance with FIPS 199 makes it difficult for DOI to select and test the most effective security controls. Furthermore, not being in compliance with FIPS 199 will make it impossible to be in compliance with the upcoming federal standard for selecting minimum security controls, known as FIPS

---

[17] Memorandum M-05-15, FY 2005 "Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," June 13, 2005, page 6, item 11.

[18] DOI uses an Asset Valuation process to assign risk levels for Confidentiality, Integrity, and Availability that was developed prior to the introduction of FIPS 199. The systems we reviewed did have designations based on the DOI Asset Valuation process. While this process was acceptable prior to FIPS 199, it is not consistent with the current standard for categorizing federal data and information systems.

200[19]. We anticipate that NIST and OMB will make FIPS 200 a federal standard and mandatory requirement for Certification and Accreditation early in calendar year 2006.

To effectively address these federal standards and OMB requirements, DOI will have to revamp its Certification and Accreditation process to ensure that it is compliant with NIST's Certification and Accreditation framework (see Appendix II) and OMB guidance. Additional areas for improvement and updating are discussed in the following sections.

Risk Assessment Findings

The risk assessment process is used to help managers and operators understand vulnerabilities and threats to their systems, consider the probability and impact of occurrence, and identify appropriate safeguards. DOI has documentation and "how-to" guides available for carrying out risk assessments; however, the majority of them are in need of updates to reflect changes in OMB guidance and NIST's Certification and Accreditation framework. DOI issued its Risk Assessment Guide[20] on April 30, 2002, which has been used for the majority of DOI's Certification and Accreditation. While the guide was published prior to NIST finalizing its Risk Management Guide[21], DOI needs to formalize the requirement to use NIST's Risk Management Guide for IT Systems (800-30) for its own risk assessments.

We found that the Bureau of Reclamation (BOR) had re-certified a system in February 2004 using a risk assessment that was nearly 2 years old. Systems that undergo recertification should also undergo a new risk assessment. We also found that the following risk assessments for NBC systems did not meet the requirements of NIST 800-30 because the risk assessments did not include a control analysis and control recommendation section:

- Consolidated Financial System (CFS/ Hyperion)
- Denver Data Center (DDC) General Support System
- Interior Department Electronic Acquisition System (IDEAS)
- Reston LAN General Support System
- ARTNET General Support System [22]

---

[19] Federal Information Processing Standard 200 (draft), "Minimum Security Requirements for Federal Information and Information Systems". July 2005.
[20] Interior Risk Assessment Guide, April 30, 2002.
[21] NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems"
[22] According to a memorandum from the NBC Bureau IT Security Manager to the OCIO on August 10, 2005, ARTNET was transitioned to the Enterprise Service Network effective August 10, 2005.

Additionally, the Federal Financial System (FFS) risk assessment did not meet the requirements of NIST 800-30 because it did not include a control analysis, likelihood determination, impact analysis, risk recommendation, or control recommendations.

An important part of DOI's risk assessment process is its asset valuation process. DOI uses an Asset Valuation Guide[23] to help those involved in the Certification and Accreditation process determine a systems value, data sensitivity, information categories, and capture other relevant information. The Asset Valuation Guide is not consistent with FIPS 199 and NIST guidance for determining security categorization levels for various types of federal data (SP 800-60[24]). We noted discrepancies for risk designation between various security documents, including the following:

- The Fish and Wildlife Service (FWS) Wide Area Network Contingency Plan notes that it "provides the entirety of network connectivity for every mission critical IT system in the Service." DOI's Asset Valuation Guide notes that Wide Area Networks – such as the FWS's – trust. and financial systems are supposed to be categorized as high risk. However, the DOI Certification and Accreditation listing states the security category of FWS Wide Area Network is low while the FWS Wide Area Network Plan of Actions & Milestones for the third quarter of FY 2005 states the system is a high. We noted that FIPS 199 is not specifically cited in any of the relevant FWS Wide Area Network security documents. Interviews with FWS staff revealed that FWS is looking to DOI for guidance.

- BOR's Wide Area Network FIPS categorization is not stated and its attempts to classify risk are inconsistent:

  o The June 24, 2005 System Security Plan makes no mention of FIPS 199.
  o The third quarter Plan of Actions & Milestones for FY 2005 states that BOR's Wide Area Network is a medium category system.
  o The Certification and Accreditation listing states BOR's Wide Area Network is mission critical and yet does not determine the security category for the system.

Security Self-Assessment Findings

Annual security self-assessments are required by FISMA and DOI policy. DOI carries out NIST 800-26[25] security self-assessments and other forms of security testing, such as scanning. We found a number of inconsistencies in this area, including the following: *r* .

---

[23] "DOI IT Asset Valuation Guideline", March 4, 2003.
[24] NIST Special Publication 800-60. "Guide for Mapping Types of Information and Information Systems to Security Categorization Levels".
[25] NIST Special Publication 800-26, "Security Self-Assessment Guide for IT Systems."

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

- The MMS Wide Area Network's NIST Special Publication 800-26 security self-assessment was incomplete, with many areas not addressed.

- The NBC's Federal Personnel and Payroll System (FPPS) NIST Special Publication 800-26 security self-assessment states that FPPS does not have any interconnections and thus interconnection agreements are not necessary. However, the FPPS system security plan lists numerous interconnections and states that the agreements are currently under development.

- The NBC's FPPS NIST Special Publication 800-26 security self-assessment states that system administrators periodically review user privileges to ensure they remain in line with duties. However, the Financial Statement Audit revealed that not all user accounts are reviewed. A Notice of Finding and Recommendation (NFR) has been issued by KPMG on this subject in this year's financial audit.

- The NBC's FFS NIST Special Publication 800-26 security self-assessment states that policy and procedures dictate system administrators perform periodic reviews of user account privileges. However, the Financial Statement Audit revealed that Office of the Secretary user accounts are not reviewed. An NFR has been issued by KPMG on this subject in this year's financial audit.

- The NBC's FFS NIST Special Publication 800-26 security self-assessment states that FFS auditing has been integrated. However, the Financial Statement Audit revealed that audit capabilities were not turned on at the Office of the Secretary application. As such, Office of the Secretary system administrators were not reviewing FFS audit trails. An NFR has been issued by KPMG on this subject in this year's financial audit.

- The NBC's IDEAS NIST Special Publication 800-26 security self-assessment states that various account management policies, procedures, and controls are integrated. However, the FY 2005 Financial Statement Audit revealed that formal account management practices were not implemented. An NFR has been issued by KPMG on this subject in this year's financial audit. This finding is repeated from FY 2004.

- The NBC's Reston LAN NIST Special Publication 800-26 security self-assessment states that management has authorized and integrated all interconnection agreements. However, we note that the lack of a signed interconnection agreement is identified as a current issue on the Reston LAN Plan of Actions and Milestones.

System Security Plan Findings

System security plans are an important part of the Certification and Accreditation process. They provide an overview of a system's security requirements and document the controls used to secure the system. We found a number of issues with the system security plans we reviewed. Several of them had not been updated to reflect current changes to the system's infrastructure. No plan we reviewed was well positioned to address NIST control requirements[26] or to be in compliance with the upcoming security control standard[27]. NIST Special Publication 800-53 helps agency system owners select the security controls for their system based on the system's FIPS 199 categorization, while FIPS 200, when finalized by the end of this calendar year, will make NIST Special Publication 800-53 a federal standard for selecting controls. System interconnections issues also continue to be weaknesses in DOI's system security plans, including the following:

- Page 11, section 2.3.3.1 of the FWS Wide Area Network system security plan states that all major applications and general support systems that are interconnected with the Wide Area Network system will sign the interconnections service agreement. These agreements have not been completed.

- Section 1.1.1 of the NBC FPPS system security plan includes information on the various interconnections of FPPS. The system security plan also includes information on the status of interconnections agreements. The plan notes that many of the agreements have not been developed and/or signed to date.

- Section 1.7 of the NBC FFS system security plan references the Denver Data Center Enclave plan for a listing of all interconnections. The FFS system security plan also notes that the interconnections are not signed to date.

- Section 1.8 of the NBC CFS system security plan states that the only true interconnection with Hyperion is to the Internet. The system security plan also states that CFS clients sign a security services agreement with the NBC. However, these agreements are not signed with all clients.

- Section 1.8 of the NBC IDEAS system security plan includes a listing of interconnected agencies and specifies the logistics of the interconnections. However, the plan does not indicate if interconnection agreements are signed.

---

[26] NIST Special Publication 800-53.[26]
[27] Federal Information Processing Standard 200.

- Section 1.6. of the mainframe portion of the NBC Denver Data Center Enclave system security plan includes a listing of all connected agencies. However, the plan does not indicate the status of interconnection agreements.

- Appendix A of the NBC Reston LAN system security plan includes a listing of the interconnected systems. However, the plan does not indicate the status of interconnection agreements.

We did note that the system security plans for the NBC that we reviewed appear to be updated periodically, but we did observe some out-of-date contact information. Specifically, we determined the following contact information has not been updated:

- An NBC employee listed as the program manager, system manager and security manager for FFS, retired from the NBC earlier in FY 2005. The same employee is listed as the program manager for IDEAS and in the Denver Data Center Enclave is listed as the system manager and security manager for the Albuquerque LAN.

- Another NBC employee is listed as the point of contact for the Reston LAN in section 4.1.1 regarding resets of passwords; however, this employee retired in FY 2004.

Security Test and Evaluation Findings

The security test and evaluation report provides validation on the effectiveness of deployed controls and is an essential component of understanding system risk. We noted that eight of the 17 systems we reviewed had security test and evaluation reports that were dated after they were accredited. NIST and DOI policy requires that these reports be completed before a system is given a full accreditation. This raises questions regarding the completeness and accuracy of the information provided to approving officials during the Certification and Accreditation process. The OIG Office of Investigations is continuing to investigate this issue as a separate matter.

System Contingency Plan Findings

IT system contingency plans are an essential component of the Certification and Accreditation process. They provide system operators with the guidance and procedures needed to recover from an emergency or system level outage. Accuracy, timeliness, testing, and consistent documentation are critical for an effective contingency plan. We observed that only 4 out of the 15 systems that need to have their contingency plans tested this year actually have updated contingency plans, making it difficult to determine what was done or the effectiveness of the test:

- The NBC Denver LAN contingency plan has not been updated since June 2004, even though NBC has migrated from Novell to Active Directory and performed two connectivity tests.

- The MMS Wide Area Network contingency plan has a number of errors, including use of "sample" data and incomplete contact information.

- The Bureau of Reclamation Wide Area Network contingency plan test was conducted on May 17, 2005. The report that was provided documenting the test does not provide any results. The report does state that the revised contingency plan will be available June 30, 2005. However, the revision history in the plan dated June, 24, 2005, does not reflect any changes to the plan and the results of the test are not noted in the test plan report or the contingency plan.

We also found that most of the NBC system contingency plans had outdated or incorrect contact information for critical individuals. In order to verify the accuracy of the team contact information provided in the contingency plan, we performed a comparison to the current NBC directory. Upon comparison, we found the following discrepancies:

- The person listed as the team leader of the emergency management team is no longer employed. The alternate point of contact remains accurate.

- Another employee listed as a member of the emergency management team and the team leader of the operations team is no longer employed. The alternate point of contact remains accurate.

- The person listed as the FPPS contact has transferred to the financial division. Additionally, this person's contact information is incorrect.

- The employee listed as the IDEAS contact resigned in FY 2004.

Plan of Actions and Milestones Findings

The Plan of Actions and Milestones is an essential component of the Certification and Accreditation process. Weaknesses within the DOI Plan of Actions and Milestones process directly affect the overall integrity and validity of DOI's Certification and Accreditation program. Our findings over the past 3 years indicate significant issues for DOI's Certification and Accreditation process, including the following:

- Clear and consistent understanding of the remaining risks, their levels and their priority for remediation efforts are needed to maintain a system's accreditation.

- Accurate and well-managed schedules for correction, resource requirements, and budgetary allocation to ensure adequate security throughout the life cycle of the system are all needed to maintain a system's accreditation.

- Overall accountability for managing the process and correcting the weakness is not well defined, is not standardized, is not well understood, and is not fully integrated into the continuous monitoring phase of the system accreditation.

DOI Certification and Accreditation Quality Assurance Findings

Also, as part of our evaluation of the Certification and Accreditation program, we reviewed the quality assurance process that evaluated Certification and Accreditation process for the OCIO in FY 2005. While DOI has implemented a quality assurance process and should be commended for these reviews, we identified several issues that need to be implemented to improve the process and ensure Certification and Accreditation stakeholders are fully aware of the quality of DOI's efforts:

- The DOI Quality Assurance program reviewed three principle Certification and Accreditation documents: the system security plan, the risk assessment, and the security test and evaluation report.[28] It did not, however, review in detail the Plan of Actions and Milestones, the system contingency plan, and DOI's asset valuation guide for each system. These documents are essential for a full understanding of the system's overall security posture.

- A critical component of any accrediting decision is understanding the risk acceptance of vulnerabilities made by the accrediting official, particularly high-risk items. The present quality assurance process lacks an independent analysis of risk acceptance.

- The quality assurance work we reviewed lacked recommendations for updating the critical Certification and Accreditation documents to reflect FIPS 199 requirements.

- When problems are discovered that require a change in the accreditation status, timely notification to appropriate officials within DOI and outside DOI – such as the Department of Justice, OMB, and the Government Accountability Office – must be made prior to reporting official Certification and Accreditation metrics.

---

[28] We found the methodology and questions used to review these three documents to be quite good, including the overall summaries. We did note, however, that some contractors provided more substantial comments and recommendations than others.

REDACTED PUBLIC VERSION
Annual Evaluation of the
Information Security Program of DoI
Page 21 of 45

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

We noted that DOI provided Certification and Accreditation-specific training in FY 2004 in the form of national workshops, but we could not determine if any training was provided in FY 2005, especially to DOI's designated approving authorities or approving officials. Given changes to OMB's Certification and Accreditation guidance and NIST's development of a robust set of Certification and Accreditation guides and standards, DOI needs to provide updated training to staff.

Security Configurations[29]

FISMA requires that each agency "develop minimally acceptable system configuration" requirements for technologies such as Windows, UNIX, and Oracle. In this year's report, OMB has asked OIGs to determine if agency-wide security configuration policies have been developed.

DOI developed guidance to assist its bureaus in implementing standard security configurations for major software deployments[30] in 2004. Our FISMA review indicates that bureaus are using various security configurations but none appear to be the ones prescribed by DOI policy. As such, we cannot provide a definitive answer to the specific OMB question due to a lack of consistency across the Department with a DOI-wide perspective on the use of security configurations, their effectiveness, or the percentage deployed for any of the agency-wide security configurations. We requested information from OCIO on this question and only received responses from 4 out of 10 bureaus. Even from those responses, we are not clear on what process is used to ensure that the bureaus' security configurations are actually deployed, are working effectively, or are integrated with the DOI-wide configuration management process.

We do have a higher level of confidence, however, for those bureaus who have fully implemented Microsoft's Active Directory[31] technology to distribute security configurations through its group policy feature. Group policy "pushes" down the security configurations for various Microsoft technologies, which are the main operating systems for workstations and servers in DOI, and allows us to audit it rather than individual servers or workstations. However, Microsoft's Active Directory is of limited or no value for non-Microsoft technologies, such as Oracle, Linux, Solaris, or Cisco IOS. Bureaus that are not using Microsoft's Active Directory, or have limited deployments, should be of particular concern to DOI, since much or all of the security configuration must be

---

[29] OMB Question C6.
[30] OCIO Directive 2004-007, "Standardized System Security Configurations", March 5, 2004.
[31] "Active Directory is a central component of the Windows environment that provides the means to manage the identities and relationships that make up network environments, allowing applications to find, use, and manage directory resources, such as user names, network printers, servers, etc."
http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx and http://www.geneous-software.co.uk/glossary.htm

carried out manually. In an environment with limited configuration management practices, this can pose additional risks to DOI's assets.

DOI's e-mail infrastructure proved to be particularly vulnerable to exploitation. In addition to inadequate encryption for Lotus Notes Internet-based passwords[32], unclear trust relationships exist amongst bureaus' Lotus Notes implementations. These trust relationships allowed us to bypass Lotus Notes access control features when using user IDs from one bureau on another bureau's e-mail infrastructure, giving us unauthorized user rights to various databases, address books, and other Lotus resources.

We also discovered Oracle configuration weaknesses during our penetration testing and in the annual Financial Statement Audit. These vulnerabilities allowed for unauthorized access to some of DOI's most sensitive systems and information. During our penetration testing, we did not observe any Oracle security configurations in use.

Network Security

In November 2004, we began penetration testing[33] of DOI's publicly accessible networks and systems. With the exception of three tests, we have been able to compromise the tested bureaus' IT infrastructure. Penetration testing carried out this fiscal year revealed significant DOI-wide configuration issues with DOI's Web applications and servers. The majority of our successful penetrations were due to vulnerabilities in the Structured Query Language[34]. These Structured Query Language vulnerabilities resulted in successful exploitation of the applications, the hosting server, and internal networks. Also, some Web servers were configured with default vendor's settings, indicating that adequate security configurations were not being used. Most troubling, we were able to access some of DOI's most sensitive information such as financial and privacy-related data. Our network security testing work is summarized in the penetration testing scorecard included as Appendix III. Major findings for our penetration testing are outlined below:

- The majority of DOI's Web applications that were tested were vulnerable to Structured Query Language injection attacks. This vulnerability is a systemic and material weakness throughout DOI.

---

[32] OIG Memorandum to DOI "Vulnerabilities in Lotus Notes R4 Password Encryption in Address Books," December 23, 2004.

[33] A form of testing conducted by skilled security engineers with little or no knowledge of DOI that attempts to identify, exploit, and document vulnerabilities that can be used to gain unauthorized access to DOI systems. This type of test tries to/replicate the actions that a hacker would undertake to compromise systems and information so that DOI can take the proper corrective steps to prevent unauthorized access.

[34] Structured Query Language is "A database sublanguage used in querying, updating, and managing relational databases; it is the de facto standard for database products." www.oneil.com/cfm/glossary.cfm

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b) (2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances

- DOI's bureaus do not have adequate demilitarized zones[35].

  o We were able to compromise systems intended for public access to gain unauthorized access to a bureau's internal networks and Intranet during our testing.

- Weak passwords, including several on system administrator level accounts, continue to plague DOI and were exploited frequently in our technical testing.

  o We were able to obtain username and passwords on bureau public resources.

- Oracle databases host some of DOI's most sensitive information, such as privacy and financial data.

  o We discovered and exploited significant configuration weakness in DOI's Oracle implementations.

- There was no separation between the various local area networks that comprise the bureaus overall network.

  o In each successful penetration, we gained access to internal networks. This allowed us to carry out our testing undisturbed, undeterred, with unfettered access to bureaus' systems, networks, and information.

- DOI's e-mail infrastructure, once compromised, proved to be particularly vulnerable to further exploitation, indicating that additional controls and a DOI-wide e-mail security configuration are needed.

- DOI's bureaus were successful in discovering our initial attacks and, for the most part, initiated the appropriate computer security incident response. However, with the exception of the USGS, none of our secondary attacks, which were the most damaging to the bureaus, were detected. In most cases, there was a time lag of several days to a week or more from detection to reporting to DOI.

- DOI has been slow to respond and implement recommendations.

  o Configuration issues identified in April were still present in July at NBC.

---

[35] A network with security devices, such as firewalls and intrusion detection systems, used to protect internal networks and systems from public networks, such as the Internet.

o Weaknesses with Lotus Notes identified in December 2004 were not conveyed agency-wide until some time in April 2005.

Computer Security Incident Response Capability[36]

FISMA requires agencies to have a formal process in place to detect, report, and respond to security incidents, notifying and coordinating with the Federal Incident Response Center. Additionally, agencies must notify and consult with law enforcement agencies and the respective agency OIG when they suspect criminal activity. DOI has established formal procedures for reporting security incidents and for sharing information regarding common vulnerabilities. The procedures require that bureaus report incidents to the DOI Computer Incident Response Center, which provides agency-wide computer and network systems incident response and coordination capability. In turn, the Response Center provides incident information to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, which is responsible for coordinating an incident response for federal agencies.

In reviews conducted earlier this year[37], we advised DOI that bureaus were not submitting all required reports on IT security incidents, including event reporting, to the Response Center per OCIO Directive 2004-005[38]. Only two bureaus, the National Park Service and the USGS, had reported consistently; two bureaus, the Office of Surface Mining and the BLM, had not reported at all: and the remaining six bureaus and offices fell somewhere in between. Earlier this year we advised DOI that its senior officials lacked incident information on a department-wide basis and that DOI had underreported incidents to the U.S. Computer Emergency Readiness Team. Since then, DOI has taken appropriate action to address this and we have seen improvements in the bureaus' reporting procedures.

However, our penetration testing has revealed other problems with DOI's Computer Security Incident Response capability. DOI's bureaus, for the most part, have been successful in detecting large scale network reconnaissance activities and have taken actions to detect and block these. In most cases, there was a noticeable time lag between detection and reporting. Unfortunately, by this time we were able to penetrate through other undetected networks. In the instances where we gained unauthorized access inside a bureau, we were not detected and had unfettered access for as long as we needed it. This indicates that there is inadequate attention being paid to suspicious network activity

r.

---

[36] OMB Question C7.

[37] NSM-EV-MOI-0012-2005 "Fiscal Year 2005 Second Quarter Information Technology Security Update in Support of the Federal Information Security Management Act," May 10, 2005.

[38] OCIO Directive 2004-005 "Reporting of Medium and Low Priority Computer Security Incidents. " December 19, 2003.

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

within internal networks. We did not observe the use of intrusion detection devices[39] within internal networks, and we did not we see any kind of real-time correlation being done between various network and security devices that would alert incident responders. As such, internal networks and assets are not only at risk from unauthorized users but also would fall under the radar of DOI's Computer Incident Response Center.

Another area for management concern is the failure to consistently notify the OIG Office of Investigations of incidents reported to law enforcement. DOI's Computer Security Incident Response Handbook and policy instructs bureau personnel to contact the OIG should a potential issue requiring law enforcement arise. To date, we are not seeing consistent adherence to this requirement as bureaus are reporting directly to local or federal law enforcement, without any notification to the OIG.

Training and Awareness[40]

DOI policy[41] requires all users of IT systems, including contractors, to receive annual security awareness training. The Departmental Manual for the IT Security program[42] also requires training for all levels of personnel involved with IT systems, including system managers, system owners, operators, IT security staff, and executives. We found that DOI provided adequate annual security awareness training to its personnel and began a new process to provide specialized training to staff with significant information security responsibilities.

However, DOI still lacks a standard way to identify all contractors with access to DOI systems and relies on contractors to self-report their annual security awareness training. Specifically we found the following:

- Through completion of fieldwork for the Federal Information System Controls Audit Manual portion of our FY 2005 financial statement audit, we determined that NBC does not have a process to monitor whether employees and contractors complete specialized IT training related to job functionality.

- During our FISMA review, we found that the NBC/Office of the Secretary contractor for the Drug Testing System had not yet taken DOI's IT security training, and the contractor had not been advised that they needed to take the course by a given date.

---

[39] An intrusion detection system inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Http://www.webopedia.com/TERM/I/intrusion_detection_system.html.
[40] OMB Questions C8 and C9.
[41] OCIO Bulletin 2002-007 "Interim Guidance for Basic End-User Information Technology Security Training and Awareness", May 13, 2002.
[42] Part 375 Departmental Manual, Chapter 19, "Information Technology Security Program", April 15, 2002.

Likewise, DOI still does not have an accurate record for all individuals with significant information security responsibilities and does not maintain a system to keep track of their training. Although some key NBC IT personnel have attended specialized training in the past year, training plans do not exist for all employees. As such, NBC cannot ensure all key IT personnel have attended appropriate training. Our audit team notes that a Notice of Finding and Recommendation was re-issued in FY 2005 regarding this issue.

In response to an FY 2004 Financial Statement Audit Notice of Finding and Recommendation, DOI has established a department-wide learning management system. This system is to provide full functionality to assign certain courses or curricula to DOI employees based on position titles. These courses would be automatically placed in individual development plans and training plans. Completion of training would be tracked, whether the training is internal or external to DOI training programs. The vendor has been chosen and migration and testing has begun. When fully implemented, this should assist DOI in managing specific, role-based training requirements.

i̅ ˎ

ƚ

Recommendations

System Inventory

1) DOI needs to fully reconcile. consolidate, and integrate its IT security system inventory with the Departmental Enterprise Architecture Repository to ensure consistency and to accurately and fully meet FISMA's system inventory requirements.

Contractor Oversight

2) DOI needs to ensure that existing IT and telecommunications contracts have been reviewed for compliance and updated as necessary to incorporate the required practices prescribed in DOI's memorandum titled. "Information Technology Security Requirements for Acquisition," issued on August 18, 2004.

Plan of Actions and Milestones

3) DOI needs to carry out the recommendations prescribed to improve DOI's Plan of Action and Milestones process in the OIG report titled. "Evaluation Report on the Department of the Interior's Process to Manage Information Technology Security Weaknesses," issued in September 2005.

Certification and Accreditation

4) DOI needs to update its Certification and Accreditation guides and process to comply with the NIST Certification and Accreditation framework and the latest OMB guidance to include the following:

   a. Use FIPS 199 to categorize systems and understand potential impacts to DOI information and information systems.
   b. Use NIST Special Publication 800-60 for mapping information types to appropriate security categorization levels.
   c. Standardize on NIST Special Publication 800-30 for risk assessments and management.
   d. Standardize on NIST Special Publication 800-53 for selecting system security controls.
   e. Standardize on NIST Special Publication SP 800-53a for testing security controls.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b) (2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances

5) DOI should improve its Certification and Accreditation quality assurance process by doing the following:

   a) Conducting the reviews prior to a system being authorized to operate.
   b) Including a thorough review of the system Plan of Actions and Milestones.
   c) Incorporating a review and analysis of the IT system contingency plan.
   d) Validating FIPS 199 compliance and ensuring that NIST Special Publication 800-53 is being used for selecting controls.

6) OCIO should provide standard, DOI-wide training to staff with Certification and Accreditation responsibilities.

7) DOI's approving officials should receive enhanced training on the Certification and Accreditation process, be well briefed prior to making an authorized to operate decision, and fully understand any risk they choose to accept.

Security Configurations

8) Implement and adhere to DOI's standard security configurations and test systems against these baselines standards for compliance.

Network Security

9) Implement the various strategic and tactical recommendations made in the OIG's penetration testing reports and associated Notices of Potential Findings and Recommendations.

Computer Security Incident Response Capability

10) Follow standard DOI procedures to report incidents with potential law enforcement implications to the OIG's Office of Investigations.

Training and Awareness

11) Establish a reliable method for identifying contractors, and DOI employees with significant security responsibilities, needing IT security training.

OMB OIG FISMA MATRIX

ι

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review agencies can:
1) Continue to use NIST Special Publication 800-26, or
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2				
		a. FY 05 Agency Systems		b. FY 05 Contractor Systems		c. FY 05 Total Number of systems		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and evaluated in the last year		c. Number of systems for which contingency plans have been tested in accordance with policy and guidance
Bureau Name	FIPS 199 Risk Impact Level	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Bureau of Indian Affairs	High						0	0					
	Moderate						0						
	Low						0						
	Not					1	0	1	1	100.0%	1	100.0%	1	100.0%
	Sub-total	0	0	0	1	0	1	100.0%	1	100.0%	1	100.0%
Bureau of Land Management	High					0						
	Moderate					0						
	Low					0						
	Not		2	0	0	0	2	100.0%	2	100.0%	2	100.0%
	Sub-total	0	2	0	0	2	2	100.0%	2	100.0%	2	100.0%
Bureau of Reclamation	High					0						
	Moderate				1	0						
	Low					0						
	Not		1			0	1	100.0%	1	100.0%	1	100.0%
	Sub-total	0	1	0	0	1	1	100.0%	1	100.0%	1	100.0%
Fish and Wildlife Service	High					0						
	Moderate					0						
	Low					0						
	Not		1	0	0	1	1	100.0%	1	100.0%	0	0.0%
	Sub-total	0	1	0	0	1	1	100.0%	1	100.0%	0	0.0%
Minerals Management Service	High				1	0						
	Moderate					0						
	Low					0						
	Not		1	0	1	0	2	100.0%	2	100.0%	2	100.0%
	Sub-total	0	1	0	1	0	2	100.0%	2	100.0%	2	100.0%
National Business Center	High					0						
	Moderate					0						
	Low					0						
	Not		7	0	1	0	8	100.0%	7	87.5%	7	87.5%
	Sub-total	0	7	0	1	8	8	100.0%	7	87.5%	7	87.5%
National Parks Service	High					0						
	Moderate					0						
	Low					0						
	Not		1	0	1	0	1	100.0%	0	0.0%	0	0.0%
	Sub-total	0	1	0	1	0	1	100.0%	0	0.0%	0	0.0%
Office of Special Trustee	High					0						
	Moderate					0						
	Low					0						
	Not		1	0	0	0	1	100.0%	1	100.0%	1	100.0%
	Sub-total	0	1	0	0	1	1	100.0%	1	100.0%	1	100.0%
Office of Surface Mining						0	0					
U.S. Geological Survey						0	0					
Other OIG Reviews:						0						
Financial Audits						0	3					
Penetration Testing						0	1					
SCADA-NCIS						0	4					
POAM						0	3					
Wireless						0						
Agency Totals	High	0	0	0	0	0	0		0		0	
	Moderate	0	0	0	0	0	0		0		0	
	Low	0	0	0	0	0	0		0		0	
	Not Categorized	0	14	0	3	0	14	17		14		14	
	Total	0	14	0	3	0	14	17		14		14	

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.

3.a. Response Categories
- Rarely, for example approximately 0-50% of the time
- Sometimes, for example approximately 51-70% of the time
- Frequently, for example approximately 71-80% of the time
- Mostly, for example approximately 81-95% of the time
- Almost Always, for example approximately 96-100% of the time

Frequently, for example approximately 71-80% of the time

3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency Response Categories: · Approximately 0-50% complete · Approximately 51-70% complete · Approximately 71-80% complete · Approximately 81-95% complete · Approximately 96-100% complete		· Approximately 81-95% complete
3.c.	The OIG generally agrees with the CIO on the number of agency owned systems.		Yes
3.d.	The OIG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency		Yes
3.e.	The agency inventory is maintained and updated at least annually		Yes
3.f.	The agency has completed system e-authentication risk assessments.		Yes

Question 4

In this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process.   Evaluate the degree to which the following measures reflect the status in your agency by choosing from the responses provided in the drop down menu.   If appropriate or necessary, include comments in the area provided below.

For 4a -4.f, the response categories are as follows:

Rarely, for example, approximately 0-50% of the time
Sometimes, for example, approximately 51-70% of the time
Frequently, for example, approximately 71-80% of the time
Mostly, for example, approximately 81-95% of the time
Almost Always, for example, approximately 96-100% of the time

4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency	· Sometimes, for example, approximately 51-70% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	· Rarely, for example, approximately 0-50% of the time*
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress	· Sometimes, for example, approximately 51-70% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis	· Rarely, for example, approximately 0-50% of the time*
4.e.	OIG findings are incorporated into the POA&M process.	· Mostly, for example, approximately 81-95% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	· Rarely, for example, approximately 0-50% of the time*

Comments: 4.a Response Sometimes – 51-70%. However we did not determine the amount of unreported IT security weaknesses that were not included in the POA&Ms. 4.b. Response Rarely 0-50% Although DOI's POA&M process for IT security weaknesses includes the development, implementation, and management of POA&M for systems, DOI does not manage the weaknesses adequately through its POA&M process. This is demonstrated by the number of weaknesses we identified that were reported as corrected, but were not corrected, that weakness descriptions and related corrective actions were not sufficient to ensure that the weakness was understood by management or that the related corrective actions would correct the weakness. 4.c Response Sometimes – 51-70%. Although DOI program officials report to the CIO on a quarterly basis, we did not find any indications that contractors were reporting security weaknesses to program officials or bureau CIOs and that these security weaknesses were being reported by the program officials on the 4.d. Response Rarely 0-50%. Although the CIO tracks and maintains POA&M activities on a quarterly basis we found little evidence that the POA&Ms are reviewed from the standpoint that weaknesses and related corrective actions were described
and should be sufficiently acted upon and that reportedly corrected weaknesses were in fact corrected. There was also little indication that the DOI CIO sufficiently reviewed POA&M activities to ensure that all known IT security weaknesses were reported on the POA&M. This is demonstrated by the acceptance of risk that can be accomplished by DOI personnel that were not the appropriate officials for accepting such risks.
4.e. Response: Mostly 80-95%. 4.f. Response: Rarely 0-50%. Currently bureaus prioritize weaknesses within system POA&Ms. However we found little evidence that DOI overall prioritizes IT security weaknesses to ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources. The only exception is that DOI did prioritize the certification and accreditation of IT systems and obtained the necessary funding for this project. Nonetheless, not all of DOI's systems have been certified and accredited and not all significant deficiencies within these accredited systems have been corrected. Additional Comments. In response to the briefing Office of Audits provided to the DOI IT Management Council in April 2005, the DOI CIO issued a Directive requiring bureaus and offices to review previously reported corrected weaknesses and certify whether those weaknesses were in fact corrected and if not corrected report the weakness. We have not verified whether this Directive has been effectively followed by the bureaus and offices.

Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans

	Assess the overall quality of the Department's certification and accreditation process. Response Categories: · Excellent · Good · Satisfactory · Poor · Failing		· Poor

Comments:

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name:

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes

Comments: OCIO Directive 2004-007, March 05, 2004, Standardized System Security Configuration

6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	Addressed in agencywide policy? Yes, No, or N/A.	Do any agency systems run this software? Yes or No.	Approximate the extent of Implementation of the security configuration policy on the systems running the software. Response choices include: - Rarely, or, on approximately 0-50% of the systems running this software - Sometimes, or on approximately 51-70% of the systems running this software - Frequently, or on approximately 71-80% of the systems running this software - Mostly, or on approximately 81-95% of the systems running this software - Almost Always, or on approximately 96-100% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or on approximately 0-50% of the systems running this software
Windows	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Solaris	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
HP-UX	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Linux	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Cisco Router IOS	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Oracle	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Other. Specify:	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software

Comments: Other: AIX, Apache Web Servers, Remote Access Servers

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	No
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: 7.b. We identified Eight (8) instances of non-compliance from November 2004 through August 2005. Training was provided.

Question 8

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

APPENDIXES

Appendix I FY 2005 FISMA System Sub Set Evaluation Findings[43]

	Bureau	System Name	FIPS 199	C&A	POA&M	Incident Reporting	Security Assessments	Security Training and Awareness	Security Configuration
1	BIA (Contractor)	Trust Asset and Accounting Management System	X	X	X			X	X
2	BLM	National Interagency Fire Center Net	X	X	X			X	X
3	BLM	BLM Enclave	X	X	X			X	X
4	BOR	Wide Area Network	X	X	X	X		X	X
5	FWS	SWAN- Service Wide Area Network	X	X	X	X	X	X	X
6	MMS (Contractor)	Minerals Revenue Management Support System	X	X	X	X		X	X
7	MMS	Wide Area Network	X	X	X	X	X	X	X
8	NPS	NPS WAN	X	X	X	X	X	X	X
9	OS / NBC (Contractor)	Drug Testing System	X	X	X			X	X
10	OS / NBC	Reston Local Area Network	X	X	X		X	X	X
11	OS / NBC	Federal Financial System	X	X	X		X	X	X

[43] When an "X" is observed, this signifies issues in our annual evaluation that have a negative impact to the overall assessment area.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b) (2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

	Bureau	System Name	FIPS 199	C&A	POA&M	Incident Reporting	Security Assessments	Security Training and Awareness	Security Configuration
12	OS / NBC	Federal Personnel and Payroll System		X	X		X	X	X
13	OS / NBC	Interior Department Electronic Acquisition System	X	X	X		X	X	X
14	OS/ NBC	Denver Data Center Local Area Network	X	X	X			X	X
15	OS/ NBC	Consolidated Financial Statement System (HYPERION)	X	X	X		X	X	X
16	OS/NBC	Alaska Regional Telecommunication Network	X						
17	OST	Wide Area Network			X			X	X

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b) (2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances

Appendix II NIST Framework for Certification and Accreditation

Managing Enterprise Risk
The Framework

National Institute of Standards and Technology

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b) (2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances
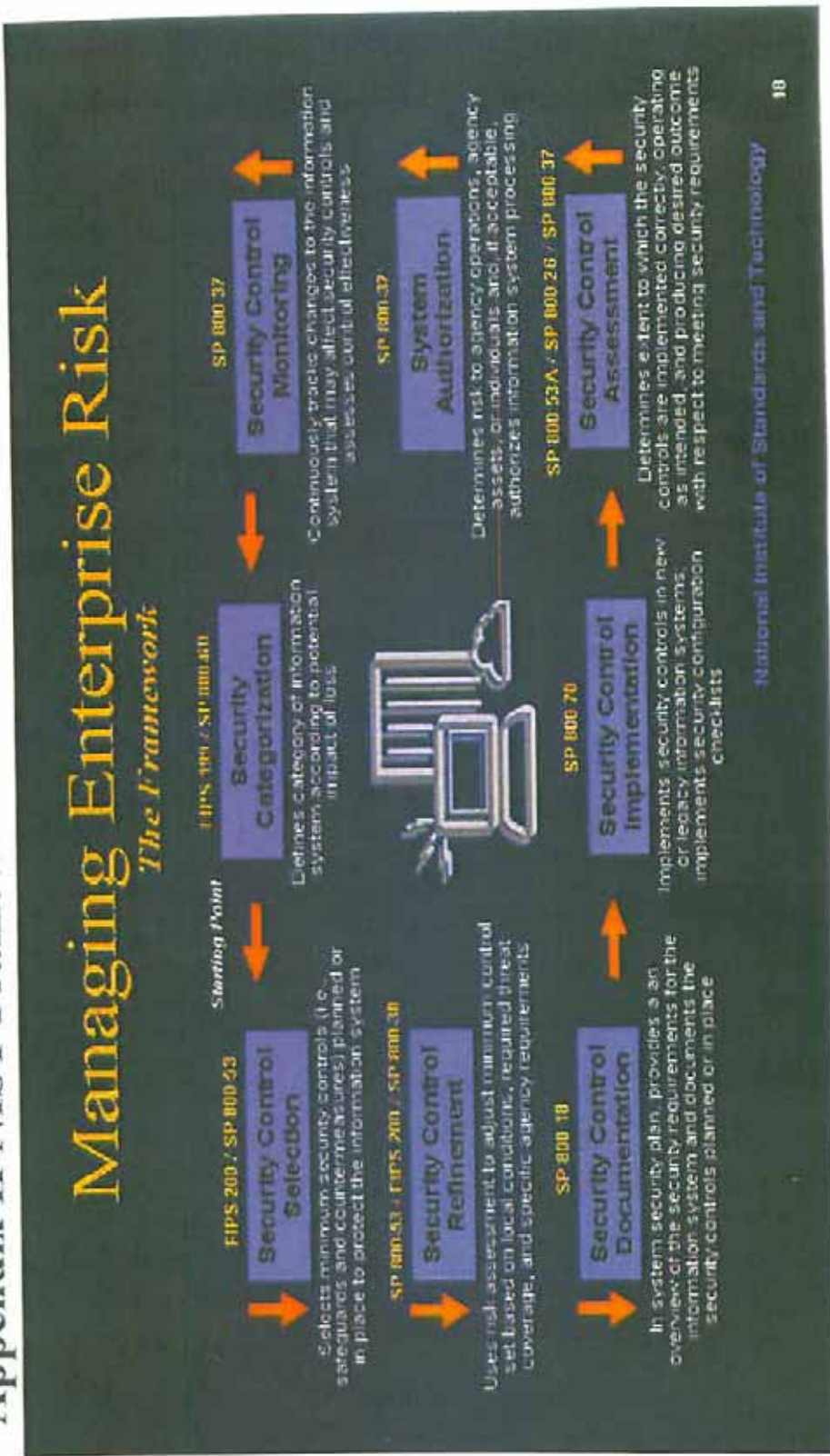
-38-

Appendix III Penetration Testing Scorecard

Bureau	Vulnerabilities	Impact	Ease of Exploitation	Overall Penetrations Risk
BIA	Limited Testing	Limited Testing	Limited Testing	Limited Testing
BLM	High	High	High	High
BOR	Medium	High	Medium	Medium
OST	Limited Testing	Limited Testing	Limited Testing	Limited Testing
USGS	High	High	Medium	High
FWS	Medium	Medium	Medium	Medium
MMS	Low	Low	Low	Low
NBC	High	High	Medium	High
NPS	High	High	High	High
OSM	Low	Low	Low	Low

Legend:
- High (orange)
- Medium (yellow)
- Low (green)
- Limited Testing (white)

REDACTED PUBLIC VERSION
Annual Evaluation of the
Information Security Program of DoI
Page 39 of 45

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

References

Laws

❖ Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) of 2002, December 17, 2002.

Office of Management and Budget Publications

❖ OMB Circular No. A-130, Management of Federal Information Resources, November 28, 2000.

Government Accountability Office Reports and Documents

❖ GAO-04-376 Information Security - Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation, June 2004.

❖ GAO-05-552 Information Security - Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements, July 2005.

❖ Federal Information System Controls Audit Manual, January 1999.

❖ GAO-04-354 Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, March 2004.

❖ GAO-04-140T Critical Infrastructure Protection: Challenges in Securing Control Systems. October 1, 2003. Testimony of Robert F. Dacey.

OIG Reports

❖ NSM-EV-BIA-0014-2005 - Testing Bureau of Indian Affairs and Office of the Special Trustee Networks from the Internet. December 10, 2004.

❖ NSM-EV-BIA-0016-2005 - Testing Bureau of Indian Affairs Offline Internet Gateway, December 23, 2004.

❖ NSM-EV-GSV-0015 and 0017-2005 External Penetration Testing of the United States Geological Service, January 3, 2005.

❖ Vulnerabilities in Lotus Notes R4 Password Encryption Address Books", issued on December 23, 2004.

❖ Evaluation Report: Department of the Interior's Use of Wireless Technologies. Report No. A-IN-MOA-0004-2004. December 2004.

❖ NSM-EV-BOR-0019-2005-Penetration Testing" External Penetration Testing of Bureau of Reclamation. March 4, 2005.

- ❖ NSM-EV-BLM-0020-2005-Penetration Testing" External Penetration Testing of Bureau of Land Management, April 6, 2005.
- ❖ NSM-EV-OSS-0025-2005-7-13-05-NBC Penetration Testing External Penetration Testing of NBC, July 13, 2005.
- ❖ NSM-EV-MOI-0003-2005-Information Security Assessment: Central Valley Operations, Sacramento, California National Critical Infrastructure Information Systems Bureau of Reclamation, September 7, 2005.
- ❖ NSM-EV-MOI-0003-2005-Information Security Assessment: Hoover Dam, National Critical Infrastructure Information Systems Bureau of Reclamation, September 7, 2005.
- ❖ NSM-EV-MOI-0003-2005-Information Security Assessment: Grand Coulee Dam, National Critical Infrastructure Information Systems Bureau of Reclamation, September 7, 2005.
- ❖ NSM-EV-FWS-0022-2005-Penetration Testing External Penetration Testing of Fish and Wildlife Service, September 7, 2005.
- ❖ NSM-EV-MMS-0021-2005-Penetration Testing External Penetration Testing of Mineral Management Service, August 5, 2005.
- ❖ NSM-EV-NPS-0023-2005-Penetration Testing External Penetration Testing of National Park Service, September 7, 2005.
- ❖ NSM-EV-OSM-0017-2005-Penetration Testing External Penetration Testing of Office of Surface Mining. September 7, 2005.BLM IT Security Penetration Testing-Notice of Potential Findings and Recommendations, April 6, 2005.
- ❖ NBC IT Security Penetration Testing-Notice of Potential Findings and Recommendations, April 19, 2005.
- ❖ NSM-EV-MOI-0012-2005 "Fiscal Year 2005 First Quarter Information Technology Security Update in Support of the Federal Information Security Management Act," January 24, 2005
- ❖ NSM-EV-MOI-0012-2005 "Fiscal Year 2005 Second Quarter Information Technology Security Update in Support of the Federal Information Security Management Act," May 10, 2005.
- ❖ NSM-EV-MOI-0012-2005 "Fiscal Year 2005 Third Quarter Information Technology Security Update in Support of the Federal Information Security Management Act," July 29, 2005.
- ❖ A-EV-MOA-0001-2005 "Evaluation Report on the Department of the Interior's Process to Manage Information Technology Security Weaknesses," August 2005.

DOI Polices, Procedures, and Other Documents

- ❖ Notification of Potential Findings and Recommendations: Confidentiality, Integrity, and Availability of Sensitive Financial and Privacy Data Managed by the NBC Is at Risk. May 05. 2005.
- ❖ Memorandum from Assistant Secretary for Policy, Management and Budget, "Penetration Testing Results at the NBC," June 15, 2005.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b) (2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any

Annual Evaluation of the
Information Security Program of DoI
-41-
Page 41 of 45

Subject to Protective Order Regarding
Sensitive I-T Security Information
(Dkt. No. 2937) (Filed April 22, 2005)

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

- Securing DOI's Network and Computer Infrastructure. Memorandum issued by DOI's Chief Information Officer on July 22, 2002.
- OCIO Directive 2004-005 Reporting of Medium and Low Priority Computer Security Incidents, December 19, 2003.
- Plan of Actions and Milestones (POA&M) Process Verification. IRM Bulletin 2005-07, issued on May 3, 2005.
- Revised POA&M Reporting Instructions. IRM Bulletin 2004-04, issued on November 24, 2003.
- Reporting of Medium and Low Priority Computer Security Incidents. IRM Bulletin 2004-05, issued on December 19, 2003.
- Standardized System Security Configuration. IRM Bulletin 2004-07, issued on March 5, 2003.
- Revised POA&M Reporting Instructions. IRM Bulletin 2004-09, issued on February 2, 2004.
- Prohibition on Use of Wireless Network Technology. IRM Bulletin 2004-18, issued on April 4, 2004.
- System Audit Logs. IRM Bulletin 2004-20, issued on July 17, 2004.
- E-Authentication Agency Ramp-up Plans. IRM Bulletin 2004-21, issued on July 6, 2004.
- Interim Guidance for Certification and Accreditation on Information Technology Systems. IRM Bulletin 2003-03, issued on April 11, 2003.
- Computer Incident Response Capability. IRM Bulletin 2003-13, issued on August 4, 2003.
- Interior Computer Security Incident Response Handbook (v1). issued on August 4, 2003.
- DOI CIO Memorandum on Peer-to-Peer file sharing restriction, issued on July 28, 2003.
- OCIO Bulletin 2002-007 Interim Guidance for basic End-User Information technology Security Training and Awareness. May 13, 2002.
- OCIO Directive 2005-007. FY 2005 Plan of Actions and Milestones (POA&M) Process Verification, May 3, 2005
- OCIO Memorandum "Implementing OCIO Directive 2005-007 for 4th Quarter Plan of Actions and Milestones (POA&M) and 4th Quarter Federal Information Security Act (FISMA) Performance Measures, August 18, 2005.
- Part 375 Departmental Manual. Chapter 19, Information Technology Security Program, April 15, 2002.
- Interior Information Technology Security Plan, Version 2, April 15, 2002.
- Interior System Security GSS Planning Guide and Template. April 30, 2002.
- Interior System Security MA Planning Guide and Template, April 30, 2002.
- Interior Risk Assessment Guide, April 30, 2002.
- Interior IT System Contingency Planning Guide, April 30, 2002.
- DOI IT Asset Valuation Guideline. March 4, 2003.

NIST Special Publications and Federal Information Processing Standards

- ❖ NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.
- ❖ NIST Special Publication 800-14, Generally Accepted Principles And Practices For Securing Information Technology Systems.
- ❖ NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.
- ❖ NIST Special Publication 800-26, Security Self-Assessment Guide for IT Systems.
- ❖ NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems.
- ❖ NIST Special Publication 800-34, Contingency Planning Guide for IT Systems.
- ❖ NIST Special Publication 800-40, Procedures for Handling Security Patches. Draft, April 1, 2002.
- ❖ NIST Special Publication 800-42, Guideline on Network Security Testing.
- ❖ NIST Special Publication 800-47, Security Guide for Interconnecting IT Systems.
- ❖ NIST SP 800-53, Recommended Security Controls for Federal Information Systems.
- ❖ NIST SP 800-60, Guide for Mapping Types of Information and Information Systems to Security Categorization Levels.
- ❖ NIST SP 800-65, Integrating Security into the Capital Planning and Investment Control Process.
- ❖ FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.
- ❖ FIPS 200 (draft), Minimum Security Requirements for Federal Information and Information Systems, July 2005

Other References

- ❖ "21 Steps to Improve Cyber Security of SCADA Networks," Joint Publication of the President's Critical Infrastructure Protection Board and the Department of Energy, September 2002.
- ❖ Practices for Securing Critical Information Assets. Critical Infrastructure Assurance Office.

Acronyms List

Abbreviations:

BIA   Bureau of Indian Affairs
BLM   Bureau of Land Management
BOR   Bureau of Reclamation
C&A   Certification & Accreditation
CSIRC   Computer Security Incident Response Capability
DM   Departmental Manual
DOI   Department of the Interior
FIPS   Federal Information Processing Standard
FISMA   Federal Information Security Management Act
FMFIA   Federal Manager's Financial Integrity Act
FWS   Fish & Wildlife Service
GAO   Government Accountability Office
MMS   Minerals Management Service
NBC   National Business Center
NIST   National Institute of Standards and Technology
NPS   National Park Service
OIG   Office of Inspector General, Department of the Interior
OMB   Office of Management and Budget
OST   Office of the Special Trustee
OSM   Office of Surface Mining
SP   Special Publication
SSP   System Security Plan
ST&E   Security test and Evaluation
USGS   United States Geological Survey
U.S.C. United States Code

System Abbreviation Names:

BIA   TAAMS   Trust Asset and Accounting Management System
BLM   BLM Enclave GSS Bureau of Land Management Enclave
BLM   NIFC   National Interagency Fire Center
BOR   RecNet   Reclamation Perimeter and Backbone Wide Area Network
FWS   SWAN   Service Wide Area Network
MMS   MRMSS   Minerals Revenue Management Support System
MMS   MMSNet   MMS Network (excludes the WAN backbone)
NBC   CFS/ Hyperion Consolidated Financial System
NBC   DDC   Denver Data Center Local Area Network
NBC   RESTON-LAN Reston Local Area Network
NBC   DC-LAN   Washington DC Local Area Network
NBC   FFS   Federal Financial System

NBC	FPPS	Federal Personnel and Payroll System
NBC	IDEAS	Interior Department Electronic Acquisition System
NBC	DTS	Drug Testing System
NPS	PARKNET System	www.nps.gov-ParkNet PIMS-Park Information Management
OST	OSTNet	OST LAN/WAN
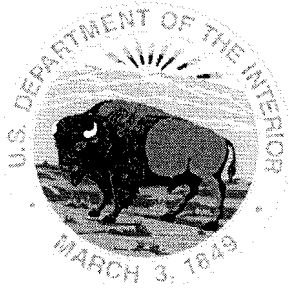
U.S. Department of the Interior
Office of Inspector General

Evaluation Report

THE DEPARTMENT OF THE INTERIOR'S PROCESS TO MANAGE INFORMATION TECHNOLOGY SECURITY WEAKNESSES

REPORT NO. A-EV-MOA-0001-2005

SEPTEMBER 2005

United States Department of the Interior

Office of Inspector General
Washington, D.C 20240

Memorandum

To: Assistant Secretary for Policy, Management and Budget

From: Earl E. Devaney
           Inspector General

Subject: Department of the Interior's Process to Manage Information Security
           Weaknesses (Report No. A-EV-MOA-0001-2005)

The attached report presents the results of our evaluation of the Department's process to manage information technology security weaknesses. We concluded that the Department had not implemented an effective plan of actions and milestones (POA&M) process and as a result, the process should be reported as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the 2005 Performance and Accountability Report. Our report presents recommendations that are designed to assist the Department in improving its POA&M process.

In the September 14, 2005 response to the draft report, the Department's Chief Information Officer did not specifically concur or non-concur with our findings and recommendations. The response indicated that the Department had fully implemented three of the five recommendations and that no further action was needed to implement the remaining two recommendations. Although we acknowledge recent steps taken by the Department to improve the POA&M process, the actions taken have not fully addressed our recommendations. Accordingly, we consider all five recommendations unresolved.

To resolve the report, we would appreciate your specific comments on actions taken or planned, including target dates and titles of responsible officials, to implement the recommendations. Therefore, as required by Departmental Manual (360 DM), please provide us with your written response to the report by October 23, 2005.

The legislation, as amended, creating the Office of Inspector General requires that we report to Congress semiannually on all audit reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented.

We appreciate the cooperation provided by the Department and agency staff during our evaluation. If you have any questions regarding this report, please call me at (202) 208-5745.

Attachment

EXECUTIVE SUMMARY

WHY WE DID THIS EVALUATION

The Office of Management and Budget (OMB) requires federal agencies to maintain a plan of action and milestones (POA&M) to assist in identifying, assessing, prioritizing, and monitoring progress to correct information technology security weaknesses found in systems and programs. The POA&M is also used to report progress on remediation efforts to correct security weaknesses to OMB and Congress. The Department of the Interior's (Department) Chief Information Officer (CIO) has stated that the POA&M is the Department's authoritative tool for managing information technology (IT) security weaknesses. The objective of our evaluation was to determine whether the Department's POA&M process was adequate.

RESULTS IN BRIEF

We found that the Department had not implemented an effective POA&M process. Specifically, our evaluation determined that the Department's POA&M:

- did not contain all known weaknesses;

- included weaknesses reported as corrected which in fact were not corrected; and

- insufficiently described weaknesses and planned corrective actions.

These problems occurred because the Department's Office of the CIO had not instituted effective quality assurance and verification processes to ensure that bureaus and offices reported complete, accurate, and reliable information. The process, as implemented, did not hold responsible officials accountable for reporting accurate and reliable information in the POA&M. Further, the process did not require weaknesses be prioritized on a Departmental basis. Additionally, the automated system used for the Departmental POA&M did not contain standardized information or provide for easy information queries or reporting, which limited its usefulness as a management tool.

As a result, the Department lacks assurance that the most critical security weaknesses are being corrected first and that its systems and data are adequately safeguarded. Furthermore, the Department is reporting inaccurate and misleading information to OMB and Congress.

In our opinion, the POA&M process should be reported as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the Department's 2005 Performance and Accountability Report.

To improve the Department's POA&M process, we recommend that all identified IT security weaknesses be reported and prioritized; the status of corrective actions be

i

monitored and verified; and responsible officials be held accountable for the accuracy of their data in the POA&M. Additionally, we are recommending that the Department upgrade its automated system to be a useful management tool.

TABLE OF CONTENTS

ACRONYMS AND TERMS

BLM	Bureau of Land Management
BOR	Bureau of Reclamation
bureau	Department of the Interior's bureaus and offices
CIO	Chief Information Officer
Department	Department of the Interior
FISMA	Federal Information Security Management Act of 2002
GS	Geological Survey
IA	Indian Affairs
IT	Information technology
MMS	Minerals Management Service
NPS	National Park Service
OIG	Office of Inspector General
OMB	Office of Management and Budget
OS	Office of the Secretary
POA&M	Plan of action and milestones

iv

INTRODUCTION

BACKGROUND

A plan of action and milestones is used to identify, assess, prioritize, and monitor the progress of corrective efforts regarding information technology security weaknesses identified in a system or a program.

The Federal Information Security Management Act of 2002 (FISMA) requires federal executive branch agencies to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency. The Office of Management and Budget (OMB) designed[1] the plan of action and milestones (POA&M) to meet this requirement.

OMB policy requires a POA&M be prepared for each system and program where information technology (IT) security weaknesses have been found. A POA&M should identify each weakness including the related corrective actions, the scheduled completion date for correcting each weakness, and the status for correcting each weakness. The Department of the Interior's (Department) bureaus and offices (bureaus) should prepare POA&Ms for each of their systems and programs where security weaknesses have been identified. The Department's Office of the Chief Information Officer (CIO), using the bureaus' data, prepares a POA&M for the Department that is submitted to OMB. In the Department's September 15, 2004 POA&M, the Department reported that it had 157 IT systems and 13 programs, that there were 2,243 IT security weaknesses, and that 883 of these 2,243 weaknesses had been corrected. The Department also reported that it would cost approximately $125 million to correct the total 2,243 weaknesses (including the funds already spent to correct the 883 weaknesses).

PRIOR REVIEWS

The Government Accountability Office has not issued any reports related to the specific objective of this evaluation. The Office of Inspector General (OIG) has issued three reports on the Department's information security program that included findings related to the Department's POA&M process. (See Appendix 1 for summaries of these findings.) In the most recent report, *Annual Evaluation of the Information Security Program of the Department of the Interior* (Report No. A-EV-MOA-0006-2004), we noted that the Department had established a POA&M process consistent with OMB guidance. However, the evaluation was limited and did not include tests to determine

---

[1] OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," issued October 17, 2001. This Guidance was updated by OMB Memorandum M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting."

whether the process was properly implemented. In that same report, we concluded that all weaknesses were not recorded in the POA&M, priorities were not assigned to correct all weaknesses, and costs for actions to remedy weaknesses were not always identified.

OBJECTIVE AND SCOPE

The objective of our evaluation was to determine whether the Department's POA&M process to manage IT security weaknesses was adequate. To accomplish our objective, we interviewed personnel involved with the process, analyzed the Department's POA&Ms of September 15 and December 15, 2004, and conducted tests of weaknesses reported as corrected. In performing our tests, we judgmentally selected 133 weaknesses in 20 IT systems and 1 security program. These systems and program were owned by the Office of the Secretary (OS), the Assistant Secretary of Indian Affairs (IA), the Bureau of Land Management (BLM), the Bureau of Reclamation (BOR), the Geological Survey (GS), the Minerals Management Service (MMS), and the National Park Service (NPS). (See Appendix 2 for more details on scope, methodology, and the criteria used in this evaluation.)

RESULTS OF EVALUATION

DEPARTMENT'S POA&M WAS NOT RELIABLE

We concluded that the Department's POA&M could not be used to effectively manage the Department's IT security weakness remediation process. The POA&M was incomplete, inaccurate, and misleading.

Known Weaknesses Were Not Reported

We found that not all known weaknesses were included in the Department's POA&M. For example, bureau staff indicated that:

> ➤ unless a weakness was determined to be "material" it would not be reported (GS and NPS).

> ➤ weaknesses were not reported (1) when identified through day-to-day operations, (2) which could be corrected within short time frames, or (3) when the security risks were determined to be low and accepted by levels of management at or below bureau IT system owners (OS, IA, BOR, GS, and NPS).

In addition, we found that the Department did not have POA&Ms in place for 11 systems that were not yet certified and accredited. Lack of certification and accreditation is a known weakness that must be addressed and should be documented in a POA&M.

Weaknesses Reported as Corrected Were Not Corrected

About half (64 of 133) of the weaknesses reported as corrected which we tested were not corrected. (See Appendix 3 for a summary of the results of the IT security weaknesses we tested.) Specifically, we determined that corrective actions were either not performed or were not sufficient to correct weaknesses. For example,

> ➤ Three corrective actions required the purchase of computer equipment, but the equipment had not been ordered.

> ➤ Nine corrective actions required that contingency plans be developed, tested, and updated, but the plans were nonexistent, were still in draft, or had not been updated.

3

> Five corrective actions required a new IT system be implemented, but the system had not been implemented.

> Seven corrective actions required the issuance of policies, but the policies issued did not adequately address the weaknesses.

> Fourteen corrective actions required that management accept the security risks associated with the weaknesses. However, the documentation supporting managements' acceptance of risk was nonexistent, did not adequately justify risk acceptance, or was not created until after our request for the documentation.

Descriptions of Weaknesses and Actions to Correct Weaknesses Were Not Adequate

In our analysis of the information reported in the Department's POA&M, we also found that weaknesses and actions to correct weaknesses were not always adequately described. Weakness descriptions such as "data integrity," "user passwords cracked," and "insufficient auditing capability" were used. For example, in a weakness described as "insufficient auditing capability" the planned corrective action was to "implement controls for sufficient auditing capability." We believe that these descriptions did not clearly convey the significance of the weakness being reported or what specific actions were planned to correct the weakness.

MANAGEMENT OVERSIGHT WAS NOT EFFECTIVE

The Department's Office of the CIO had issued some policies and procedures regarding the POA&M process. However, the Office did not oversee the process to ensure that the Department's POA&M could be used to effectively manage IT security weakness remediation and was accurate, timely, and resulted in safeguarding IT resources. Specifically, the Office of the CIO did not institute adequate quality assurance and verification methodologies and did not require that responsible officials, such as bureau heads, be accountable for the accuracy of reported information and for correcting IT security weaknesses. The Department's CIO also had not instituted an effective process to ensure that weaknesses were prioritized based on the risk to the Department. In addition, the Department's Office of the CIO had not ensured that the automated system used for the POA&M could be used as an effective management tool.

No Quality Assurance Process

The Office of the CIO had not established an effective quality assurance process to review information submitted in the bureaus' quarterly POA&Ms to ensure accurate and complete information was included in the Department's POA&M. Although the Office of the CIO performed a limited review of the count of weaknesses reported by the bureaus, this review was not comprehensive and did not ensure that (1) all systems in the Department's IT system inventory were included; (2) IT security weaknesses were clearly described so that weaknesses were understood; and (3) reported planned corrective actions would correct the weaknesses. For example, the Department's September 15, 2004 POA&M:

> Did not include an Office of Surface Mining Reclamation and Enforcement (OSM) system. This happened because OSM did not include the system in its quarterly submission to the Department and the Department did not compare OSM's submission to the Department's IT system inventory to ensure completeness.

> Included more than 300 vague or incomplete IT security weakness descriptions. These vague descriptions included nine U.S. Fish and Wildlife Service (FWS) weaknesses of "contingency plans," four BOR weaknesses of "insufficient auditing," and an MMS and an NPS weakness of "auditing." The Department did not request clarification from the bureaus for vague descriptions.

> Included approximately 700 IT security weaknesses that did not have sufficient planned actions that would correct the respective weaknesses. For these weaknesses, all of the bureaus reported that only one corrective action was planned, such as to implement a policy but did not include information describing how the policy would be implemented. For example, a BLM IT security weakness was described as the lack of separation of duties among security and administration personnel. The planned corrective action did not identify what would be done to separate the duties. Rather, the only planned corrective action was to report the weakness to a CIO Council. The Department did not require bureaus to clarify planned corrective actions.

5

Without a quality assurance process, the Department's CIO is not able to improve the quality and reliability of the Department's POA&M and the Department cannot ensure that its POA&M process is effective.

No Verification Process

We found that the CIO relied on bureaus to develop and maintain the documentation supporting corrected weaknesses and did not have a process to verify that actions were taken as reported. When we reviewed bureau procedures, we found that bureau IT security weaknesses were often considered corrected based on individuals stating they had corrected the weaknesses. The bureaus did not verify that weaknesses were corrected or that documentation, such as a cost benefit analysis had been prepared to support acceptance of risk. Therefore, the Department's September 15, 2004 POA&M inaccurately reported that weaknesses were corrected. Further, this process did not prevent IT security risks from being accepted inappropriately. For example:

> MMS had reported that 15 security weaknesses for one of its systems had been corrected; however, in our tests of the 15 reportedly corrected weaknesses, no supporting documentation existed to demonstrate that the corrective actions were implemented and tested. Further, we determined that 8 of these weaknesses had not been corrected.

> BOR reported that a security weakness for one of its IT systems was "insufficient user access controls." BOR reported that the weakness would not be corrected because "management accepted risk." BOR planned to accept the risk because (1) there were limited controls available in the system and (2) BOR would limit the number of users with direct access to the system through Rules of Behavior and oversight.

> BOR's documentation was not sufficient to support the acceptance of the risk because it did not include information such as a cost-benefit analysis or an adequate description of the planned mitigating controls such as oversight. The documentation also did not identify the position and title of the individual deciding to accept the risk.

6

Without a verification process, the Department has little assurance that its IT security weakness remediation process is effective. Appendix 4 describes good bureau practices that we believe could also be used by the Department as part of a verification process.

Inappropriate Accountability for Accurate Information in POA&Ms

Bureau heads and bureau IT system owners were not accountable for true and accurate security weakness information. Instead the Department CIO had established inappropriate accountability for reporting accurate and reliable information in the bureaus' POA&Ms. The responsibility was placed on organizations that originally identified the weakness, which could include the OIG or contractors. For example, we were told by the IA's Deputy for IT Security and Privacy that its contractors' were responsible for accurate IT security weakness descriptions in IA's POA&Ms. Neither the OIG nor contractors should be responsible for the accuracy of the Department's and bureaus' POA&M data. We believe that accountability should be established through a certification process where appropriate bureau officials, such as bureau heads, certify that POA&M information is accurate.

Weaknesses Were Not Prioritized Departmentwide

The Department's POA&M process required that weaknesses be prioritized only at the bureau level rather than Departmentwide. That is, the Department CIO did not always intervene in the prioritization of IT security weaknesses to ensure that the most critical weaknesses to the Department's mission and goals were corrected first. Consequently, we found that medium priority weaknesses for less critical systems were being corrected before high priority weaknesses for more critical systems. For example, two medium priority security weaknesses in an Office of the Secretary business essential IT system were corrected before two high priority security weaknesses of an MMS mission critical IT system.

Automated POA&M Information System Not Effective

Bureau staff indicated that the Department's automated POA&M system was difficult to use and that usable information could not be produced.

The Department's automated POA&M system could not be used to monitor, prioritize, and report on IT security weaknesses. For example, the Department's automated system, as it was implemented, does not:

> contain standardized descriptions of weaknesses and related corrective actions so that the Department could accurately prioritize all the weaknesses;

> allow for monitoring the status of specific weaknesses without extensive searching through the system;

> allow for querying information for management purposes; or

> produce a report that could be submitted to OMB without extensive editing.

Because of deficiencies in the current automated POA&M system, one bureau implemented its own system and other bureaus manually prepare their POA&M information. Generally, bureau system personnel gather and organize the information for weaknesses related to their IT systems based on bureau practices. The system personnel then submit the information to the bureau POA&M coordinator who compiles the POA&M information for all of the bureau's systems. Each bureau then submits its POA&M information to the Department. The Department must manually compile this information on approximately 2,200 weaknesses with about 2,900 corrective actions from at least 170 IT systems and programs. This compilation process begins almost 2 months before the information is sent to OMB and is repeated by the bureaus and the Department on a quarterly basis. This is not cost effective for the Department and needs to be addressed before each bureau implements its own automated system. In Appendix 4, we describe capabilities we found in reviewing POA&M automated tools at IA and the Environmental Protection Agency that the Department could use to improve its POA&M system.

THE DEPARTMENT LACKS ASSURANCE ITS IT SYSTEMS ARE SECURE

The Department's CIO has stated that the POA&M is the Department's tool to manage IT security weaknesses. As such, the Department is relying on information that we found to be inaccurate, incomplete, and untimely. Without reliable information in the POA&M, the Department cannot identify

8

systemic problems and monitor corrective actions. Also, management may make inappropriate decisions regarding the Department's information security program. Therefore, the Department cannot ensure that the most significant weaknesses are corrected first and that its systems and data are adequately safeguarded.

If the Department does not correct its process, it will continue to provide inaccurate and incomplete information to OMB and Congress. The Department should report this condition as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the Department's 2005 Performance and Accountability Report.

9

RECOMMENDATIONS, DEPARTMENT OF THE INTERIOR'S CHIEF INFORMATION OFFICER RESPONSE, AND OFFICE OF INSPECTOR GENERAL REPLY

In the September 14, 2005 response, the Department's Chief Information Officer (CIO) did not specifically concur or non-concur with our findings and recommendations. The response indicated that the Department had fully implemented recommendations 1, 2, and 3, and that no further action was needed to implement recommendations 4 and 5. Overall, the CIO stated that it had addressed all recommendations, eliminating any need to elevate concerns to the level of material weakness for this fiscal year.

Although we acknowledge recent steps taken by the Office of the Chief Information Officer (OCIO) to improve the POA&M process, we continue to believe that the current process needs to be improved and that the POA&M process should still be reported as a material weakness. Based on the CIO response, we consider all five recommendations unresolved.

We recommend that the Department Chief Information Officer, considering the bureau and the Environmental Protection Agency promising practices in Appendix 4:

Recommendation 1

Institute a quality assurance process to ensure:

      a.   all weaknesses are reported.

      b.   weaknesses are completely described and the respective corrective actions would adequately correct the weaknesses. This could be partially addressed through establishing standardized descriptions of common weaknesses and related corrective actions.

DOI Response

The Department described additional quality assurance processes in place as a result of our evaluation that it believes fully implements this recommendation. Specifically,

- The Department issued guidance requiring "Each IT security weakness identified in any review of a program or system must be entered on the authoritative POA&M..."

10

- The Department initiated a quality assurance process through OCIO Directive 2005-007 dated May 3, 2005 in which the Department stated that all bureaus complied. The Department refined and clarified its procedures in an August 18, 2005 memorandum. Additional guidance in a new OCIO Directive and POA&M Process Standard for implementation in FY 2006 will further enhance the POA&M processes.

- The Department also noted that OMB 04-25 does not require sensitive weakness descriptions, but endorses the use of general or brief descriptions. Separate source documents and reports should detail more fully information provided in the POA&M.

OIG Reply

The Department has taken recent steps to improve the POA&M process including the issuance of more detailed guidance. However, we believe that further steps are needed to implement an effective quality assurance process. While the recent guidance communicates the requirement to include all weaknesses in the POA&M, it does not describe a Department level quality assurance process to ensure that all weaknesses are actually reported. The working draft Plan of Actions and Milestones Process Standard does state that the Department Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) will be required to review the POA&Ms to ensure compliance with policies and procedures. The CISO will also be responsible for instituting a quality assurance process to ensure all systems are accounted for, weaknesses are adequately described, and corrective action plans appropriately address the weakness. However, these Standards will not be implemented until fiscal year 2006.

We agree that OMB M 04-25 endorses the use of brief descriptions and found that the OMB examples provided enough detail to understand the weakness. However, in our evaluation we identified weakness descriptions that did not meet OMB requirements. A quality assurance process would ensure weakness descriptions are adequate.

We consider this recommendation unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

11

Recommendation 2	*Institute a verification process to ensure that weaknesses reported as corrected are, in fact, corrected; that supporting documentation is maintained; and that management's acceptance of risk is appropriately justified and documented.*
DOI Response	The Department described an additional quality assurance process and verification process that it has put in place as a result of our evaluation that they believe fully implements this recommendation. The Department specifically cites OCIO Directive 2005-007 with which it states that all bureaus complied. The bureaus and offices provided verifications that weaknesses that were reported as corrected were in fact corrected. The Department plans to issue an additional Directive and POA&M Process Standard for implementation in 2006 to provide further process guidance. The POA&M Process Standard will provide for an additional quality assurance process, to be performed by the OCIO, which will include inspection and review of a sample set of completed POA&M corrective actions each fiscal year. The Department also stated that it is not cost effective to complete a cost-benefit analysis for every security weakness in which the risk is accepted.
OIG Reply	The Department has taken some steps to improve the verification process including the requirement that the bureaus conduct verifications that the weaknesses reported as corrected were in fact corrected. However, the continued reliance on self reporting by the bureaus makes compliance verification virtually impossible from a Department-wide management standpoint. In its response, the Department indicated that the Plan of Actions and Milestones Process Standard would provide for an additional quality assurance to be performed by the OCIO which will include an "inspection and review of a sample set of completed POA&M corrective actions each fiscal year." However, the current draft does not include this additional process. The Department will not have an effective POA&M process until these verification reviews are established and implemented. Additionally, we included the cost benefit analysis in our report as a promising practice that could be used by the Department in its POA&M process.

We consider this recommendation unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

Recommendation 3	*Require senior bureau management to certify that information in the bureaus' POA&Ms is accurate and true. In the certification, bureau management should acknowledge that each POA&M includes all known weaknesses, that weaknesses are adequately described, that corrective actions would adequately correct the weaknesses, and that completed actions are in fact completed."*
DOI Response	The Department responded that the quality assurance and verification process initiated by the OCIO Directive 2005-007 and further clarified in a memorandum dated August 18, 2005 requires senior management officials to ensure and verify information in the bureau's POA&M is accurate. The Department believes the implementation of the verification process fully implements this recommendation.
OIG Reply	The Department requires that remediation actions be certified by the applicable system owner and documented. We received certification statements for some of the bureaus' system POA&Ms. The certification statements only certified the completion of corrective actions to correct weaknesses, it does not certify that all known weaknesses are reported and that all required milestone tasks are included. Our recommendation was intended to require bureau officials to certify the **entire** POA&M and not just those weaknesses that were completed. We revised our recommendation accordingly. Based on the Department response, we conclude that this recommendation is unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.
Recommendation 4	*Institute a practice to review all Department IT system and program weaknesses to ensure the most critical weaknesses for the most critical systems of the Department are being addressed first.*
DOI Response	The Department did not agree with this recommendation. The Department stated that the IT budget is under the authority of multiple appropriations and with specific restrictions on the movement of appropriated funds. Thus, prioritization across bureaus is not a relevant issue. Additionally, the Department makes the following points:

- NIST SP 800-57 requires the Designated Approving Authority (DAA) to make the final decision and be held accountable for accepting risks to their systems. Having higher levels of management make changes to the

13

DAA's determination would undermine the DAA's authority and accountability.

- Interior prioritizes corrective actions as indicated by the "Scheduled Completion Date" column.

- Sequential prioritization based on risk level alone does not make sense in an operational and budgetary context where some weaknesses are more easily and quickly corrected than others. Adhering to a strictly sequential work-off plan could leave a larger number of weaknesses unresolved, which could increase the overall risks to individual systems, potentially raising the system risk to unacceptable levels.

OIG Reply

We recognize that there are budgetary restrictions prohibiting movement of funds between bureaus in most cases. However, we were made aware that the Department has available funds to address certification and accreditation of bureau and office systems. The Department can use the POA&M as a management tool in setting priorities for allocating these funds Department-wide and ensuring the most critical weaknesses for the most critical systems are being addressed first.

Based on the Department response, we conclude that this recommendation is unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

Recommendation 5

Implement an effective automated POA&M system. This can be accomplished by either improving the current system or implementing a new system. In establishing an effective system, the Department should define the requirements based on consultation with bureaus' IT operational staff, system owners, program managers, and others that are involved with the IT security weakness remediation process and canvass other federal agencies for best practices.

DOI Response

The Department recognizes the benefits of using POA&M automation tools and plans to evaluate tools for prospective use in the Department. They may not be able to immediately implement the recommendation or find it cost effective to do so. The Department believes that the current POA&M reporting format, while not optimal, meets basic requirements. A new automated POA&M system could not be funded until fiscal year 2008. The Department stated that the implementation of a single-purpose system for POA&Ms would not be beneficial because the functional requirements, such as automation of forms and workflow, are common to other Departmental and OCIO processes. Those requirements should be met with common software service components.

OIG Reply

The Department already has an automated POA&M system. Our review identified numerous deficiencies which resulted in one bureau purchasing and implementing its own system and other bureaus manually preparing their POA&M information. This is not cost effective for the Department. Our recommendation was intended to encourage the Department to improve its automated system to prevent the need for bureaus to manually prepare the information and allow for a unified Departmental process. This can be accomplished through either improving the current system or the implementation of a replacement system. In making its decision, the Department should take into consideration best practices used within the bureaus and by other federal agencies. We revised our recommendation to focus on the Department's need to identify the requirements of an effective POA&M system.

Based on the Department response, we conclude that this recommendation is unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

OFFICE OF INSPECTOR GENERAL
PRIOR REPORTS WITH FINDINGS RELATED TO THE
DEPARTMENT OF THE INTERIOR'S PLAN OF ACTION AND MILESTONES

REPORTS	FINDINGS	SUGGESTED IMPROVEMENTS AND RECOMMENDATIONS
ANNUAL EVALUATION OF THE SECURITY PROGRAM AND PRACTICES OVER NON-NATIONAL SECURITY SYSTEMS, U.S. DEPARTMENT OF THE INTERIOR (Report No. 2002-I-0049)	We noted the following deficiencies in the Department of the Interior's (Department) and the bureaus' and offices' (bureaus) July 31, 2002 plans of action and milestones (POA&Ms) to correct information technology (IT) security weaknesses: • Specific weaknesses were grouped together as overall general weaknesses. • System weaknesses were rolled into one weakness and incremental steps to address the specific system weaknesses were not included. • Only a final completion date was given for corrective actions that involved multiple years. Incremental milestone dates had not been established to effectively measure progress. • Milestone dates or resources required to accomplish corrective actions were not always presented.	• Hold program officials accountable for carrying out their information security responsibilities. • Hold subordinates of bureau heads accountable for fulfilling their information security responsibilities. • Establish a process to validate that all bureaus have effectively implemented federal and Department security policies and procedures, standards, and guidelines for all systems. • Include in the POA&Ms all necessary steps and specific completion dates.
ANNUAL EVALUATION OF THE INFORMATION SECURITY PROGRAM OF THE DEPARTMENT OF THE INTERIOR (Report No. 2003-I-0066)	Overall, POA&Ms developed by bureaus were not complete or used effectively. Specifically, the POA&Ms did not: • Include all IT systems owned and operated by the Department that had weaknesses. • Include all weaknesses whether identified through the organization's internal reviews or by organizations such as the Office of Inspector General. • Include incremental steps for correcting weaknesses especially when milestone dates were in excess of 6 months. • Always include costs for correcting weaknesses. • Prioritize weaknesses in order of significance. Also, costs identified in the POA&Ms to correct security weaknesses were not always included in bureau capital investment plans.	• Include tests to validate that information reported by bureaus is adequate and that controls are operating as planned or intended in the Chief Information Officer's (CIO) information security program reviews of bureaus. • Require that POA&Ms contain detailed steps for correcting reported weaknesses when the milestone dates exceed 6 months. • Ensure that POA&Ms include all costs necessary to correct reported weaknesses, establish priorities, and integrate costs into the IT investment plans. • Require each bureau to present to the CIO a strategic plan with incremental steps to achieve an institutionalized information security program that meets the requirements of the Federal Information Security Management Act (FISMA). The

REPORTS	FINDINGS	SUGGESTED IMPROVEMENTS AND RECOMMENDATIONS
		strategic plan should encompass the corrective actions in the POA&Ms and should be approved by the CIO.
ANNUAL EVALUATION OF THE INFORMATION SECURITY PROGRAM OF THE DEPARTMENT OF THE INTERIOR (Report No. A-EV-MOA-0006-2004)	The Department established a POA&M process consistent with Office of Management and Budget (OMB) guidance. We found that bureaus recorded known weaknesses in their POA&Ms most of the time. However, we also found a need to ensure that all weaknesses are reported, priorities are assigned to correct all weaknesses, and costs of actions needed to remedy weaknesses are always identified. Specifically, we found: • Agreed-upon weaknesses identified during Office of Inspector General (OIG) audits of bureau financial statements were not always included in the POA&Ms. • Bureaus did not incorporate all weaknesses identified through risk assessments and security tests and evaluations into their POA&Ms. • Remediation activities were not prioritized in the POA&Ms. • Resources were not always allocated based on prioritization of the weaknesses. • Resources required to complete remedial actions were not tied to budget documents. • POA&Ms did not include all of the weaknesses in a system.	The Department CIO should institute an oversight process to ensure bureaus effectively implement the Department's security program requirements. Specifically, the CIO must ensure that: • POA&Ms not only reflect prioritization of weaknesses but also identify the resources necessary to address the higher prioritized weaknesses so that the corrections of high priority weaknesses are performed first; • budget documentation and POA&Ms can be directly correlated through OMB project/system identifiers to ensure funding addresses security weaknesses; and • weaknesses identified during OIG and other internal or external reviews are included in the applicable POA&Ms at the time the weaknesses are identified and agreed to by the bureau.

SCOPE, METHODOLOGY, AND CRITERIA

We conducted our evaluation in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency. Our review was conducted from November 2004 through April 2005. To accomplish our objective, we:

> ➤ interviewed Department of the Interior (Department) and bureau and office (bureau) personnel involved in the plan of action and milestones (POA&M) process, including Chief Information Officers (CIO), information technology (IT) security managers, POA&M coordinators, and IT staff;

> ➤ reviewed the Department's and the bureaus' policies and procedures related to reporting IT security weaknesses and remediation activities on the POA&Ms;

> ➤ analyzed bureaus' IT systems and program quarterly POA&Ms that were submitted to the Department and the Department's quarterly POA&Ms that were submitted to the Office of Management and Budget (OMB) dated September 15 and December 15, 2004;

> ➤ identified practices within the Department and at other federal agencies to determine if methodologies are available to the Department for improving its POA&M reporting and remediation processes.

We also conducted tests of corrective actions for weaknesses reported as corrected in the POA&Ms. The Department's September 15, 2004 POA&M reported 157 IT systems and 13 programs with a total of 883 corrected weaknesses. The bureaus had reported to the Department for the same period 173 systems and 13 programs with 923 corrected weaknesses. We chose to select our sample from the bureaus' POA&Ms because these contained more detail. From the universe of 923 reportedly corrected weaknesses, we judgmentally selected weaknesses to test using the following methodology:

> ➤ We excluded financial and financial-related applications because the respective weaknesses are subject to review during the annual financial statements audits.

> ➤ We chose weaknesses that were related to access controls because of the significance of these controls in safeguarding IT resources and data and because these controls are included in most types of IT systems.

Based on this methodology, we identified an initial universe of 139 reportedly corrected IT security weaknesses for 39 IT systems and 1 program. Next we judgmentally selected 39 weaknesses in 18 systems and 1 program to test. We expanded our testing to include other weaknesses reported as corrected in the bureaus' POA&Ms of September 15 and December 15, 2004, for 6 of the 18 systems selected. We also included two additional IT systems with corrected weaknesses owned by the Office of the Secretary to ensure our review adequately covered the Departmental level process. In total, we tested 133 reportedly corrected weaknesses of 20 IT systems and 1 program. These systems and program were owned by the Office of the Secretary, the Assistant Secretary of Indian Affairs, the Bureau of Land

Management, the Bureau of Reclamation, the Geological Survey, the Minerals Management Service, and the National Park Service. (See Appendix 3 for the specific systems tested.)

EVALUATION CRITERIA

Public Law 107-347

Federal Information Security Management Act of 2002 (FISMA). This Act requires federal executive branch agencies to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices.

Office of Management and Budget Circular and Memoranda

Circular A-130 "Management of Federal Information Management Resources." This Circular among other issues related to IT states that:

- Application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures and work processes that improve the effectiveness and efficiency of federal agencies.
- Planning for information systems should include intended uses of the system, budgeting, and acquisition.
- Government information should be protected commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.
- Sufficient information should be recorded, preserved, and made accessible to ensure the management and accountability of agency programs.
- Improvements to existing information systems and the development of planned information systems should not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector.
- A selected system or process should maximize the usefulness of information and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information.
- IT needs should be met through cost effective intra-agency and interagency sharing before acquiring new IT resources.
- The agency head should appoint a Chief Information Officer who must report directly to the agency head to carry out the responsibilities of the agency. The Chief Information Officer must be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources.

19

- The agency head should direct the Chief Information Officer to monitor agency compliance with the policies, procedures, and guidance in this Circular. The Chief Information Officer should develop internal information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular.

Memorandum M-03-19, "Reporting Instructions for the Federal Information Security Management Act [FISMA] and Updated Guidance on Quarterly IT Security Reporting." This Memorandum describes the requirements for quarterly IT security reporting through OMB's POA&M. This guidance is applicable to POA&M reporting during fiscal year 2004.

Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act" **(FISMA).** This Memorandum describes the requirements for quarterly IT security reporting through OMB's POA&M. This guidance is applicable to POA&M reporting during fiscal year 2005.

Department of the Interior Policy and Guidance

Departmental Manual (375 DM 19) "Information Technology Security Program." This Manual chapter establishes policies, assigns organizational and management roles and responsibilities, and establishes minimum requirements for the development, implementation, maintenance, and oversight of an IT security program for protecting the Department's information and IT systems that store, process, or transmit unclassified information.

IRM [Information Resources Management] Directive 2004-009 "Revised Reporting Instructions for DOI's POA&M." This directive includes the Department's timelines for fiscal year 2004 POA&M reporting. In addition, the directive includes attachments that describe the Department's POA&M process and reporting guidance.

Instructions for POA&M Reporting. The Department provided an Excel spreadsheet with instructions for each data field to the bureaus for POA&M reporting.

Summary Results of Weaknesses Tested from Bureaus' Plans of Actions and Milestones, September 15, 2004 and December 15, 2004

Bureau and System Plans of Action and Milestones	Number of Corrected Weaknesses Reported	Number of Corrected Weaknesses Tested	Number of Corrected Weaknesses Determined Not Corrected
Office of the Secretary Security Program Aircraft Management Local Area Network General Support System (AM LAN) Alaskan Regional Telecommunications Network (ARTNET) Denver Data Center General Support System Enclave (DDCGSS) Interagency Aircraft Services Local Area Network General Support System (IAS LAN) Quarters Management Information System (QMIS) Reston Local Area Network General Support System (Reston LAN) Safety Office Local Area Network (SO-LAN)	104	15	12
Assistant Secretary of Indian Affairs Asset Management System (AMS) Educational Native American Network 2 (ENAN-2) Fee to Trust (FTT)	26	16	8
Bureau of Land Management BLM Enclave General Support System	30	20	5
Bureau of Reclamation Denver Office General Support System (DOGSS) Columbia Basin Supervisory Control and Data Acquisition (CBP SCADA) Hydrological and Meteorological Information System (HMIS) Mid-Pacific Regional General Support System (MPGSS) Safety and Security Information System (SSIS)	48	17	6
Geological Survey National Map	81	40	21
Minerals Management Service Technical Information Management System (TIMS) MMS Network (MMSNet)	23	16	8
National Park Service NPS One General Support System	32	9	4
Total	344	133	64

21

POA&M PRACTICES AND AUTOMATED SYSTEM CAPABILITIES FROM DEPARTMENT OF THE INTERIOR BUREAUS AND THE ENVIRONMENTAL PROTECTION AGENCY

During our evaluation we identified promising practices that we believe could be used by the Department of the Interior (Department) to improve its plan of action and milestones (POA&M) process. We also identified capabilities from two automated systems that would improve the Department's automated POA&M system.

AREA	PRACTICE
Documenting management accepted risks of security weaknesses.	The Bureau of Reclamation's (BOR) "System Security Risk Acceptance Form" provides a standard template for senior management to document acceptance of low risk weaknesses. Low risk weaknesses are those that do not impact the certification and accreditation that the system adequately safeguards data or that do not adversely impact operations. BOR's guidance, as it relates to the Form, requires that the information technology (IT) system owner, regional IT security manager, and BOR's Chief Information Officer review accepted security weaknesses no less than annually. The Minerals Management Service includes a cost/benefit analysis as part of its justification for acceptance of risk.
Keeping system owners updated on the status of security weaknesses.	The National Business Center's IT Security Manager sends a monthly POA&M report to system owners. The report shows the status of the corrective actions for IT security weaknesses that are ongoing and on target for completion and of each weakness that is ongoing but not on target for completion.
Using POA&Ms as a management tool at all levels in a bureau.	For one of the Bureau of Land Management's (BLM) IT systems, "working POA&Ms" are maintained for subsets of the system. In this case there is a subset for each of BLM's 13 state offices. Each "working POA&M" has a description of each weakness in that subset's part of the system as well as a description of the respective corrective actions. Each state office uses the "working POA&M" to manage the IT security weaknesses in its state. BLM, because the subset weaknesses have common identifiers, uses the "working POA&Ms" to prepare BLM's quarterly POA&M which is submitted to the Department.

As part of our evaluation, we interviewed personnel from the Assistant Secretary for Indian Affairs and the Environmental Protection Agency who demonstrated effective capabilities in their automated POA&M systems that the Department could use to improve its automated POA&M system.

CAPABILITY	DESCRIPTION
Classify IT systems as either a major application or a general support system.	The POA&M system asks questions that when answered by the user the system helps the user to classify the IT system as either a major application or a general support system. A major application requires a different set of controls than a general support system to safeguard information.
Identify weaknesses and update POA&M.	The POA&M system contains the National Institute of Standards and Technology's Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, self-assessment questionnaire. At the same time as the user completes the questionnaire, the system automatically identifies weaknesses and updates the POA&M.
Track requirements for an IT system to be certified and accredited as adequately protecting data.	The POA&M system tracks whether a system meets the requirements for it to be certified and accredited as adequately safeguarding data. These requirements include: the system must have undergone a risk assessment, the system must have undergone a self-assessment, the system must have a security plan describing all the controls that protect the system, and the system must have a contingency plan to recover in the event of a system failure or disaster.
Associate controls to applications supported by a general support system.	The POA&M system associates the controls in a general support system to the major applications supported by that general support system.
Contains standardized data on security weaknesses.	The POA&M system contains standardized descriptions of weaknesses and related corrective actions. When necessary unique weaknesses can also be added to the system.
Tracks the completion of corrective actions.	The POA&M system tracks the completion of corrective actions for standardized weaknesses. The system ensures that the scheduled corrective actions are in an appropriate order and does not allow weaknesses to be reported as corrected before all information supporting the completion of the corrective actions has been input into the system.

23

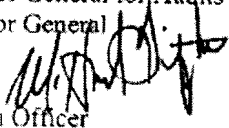| CAPABILITY	DESCRIPTION
Allows queries of weakness data.	The POA&M system allows queries to obtain data regarding IT security weaknesses including the progress of corrective actions. In addition, the system can generate POA&M reports in OMB's required format.
Maintain history of weaknesses.	Maintains records of weaknesses that were corrected and allows corrected weaknesses to be re-opened if necessary.
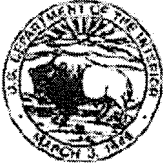
United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, DC 20240

TAKE PRIDE
IN AMERICA

Memorandum   SEP 14 2005

To: Assistant Inspector General for Audits
             Office of Inspector General

From: W. Hord Tipton
             Chief Information Officer

Subject: Response to "Draft Evaluation Report on the Department of the Interior's
             Process to Manage Information Technology Security Weaknesses
             (Assignment No. A-EV-MOA-0001-2005)."

Thank you for the opportunity to respond to the "Draft Evaluation Report on the
Department of the Interior's Process to Manage Information Technology Security
Weaknesses (Assignment No. A-EV-MOA-0001-2005)." The Plan of Action and
Milestones (POA&M) process is a vital component of the Department's Information
Technology (IT) security program. As you know, Interior made significant progress in
establishing and implementing a department-wide POA&M process, to the point where
the Office of Inspector General concluded in 2004, "Based on our examination of the
Department's instructions for the development and implementation of POA&Ms, we
concluded that as designed, the POA&M process is effective and satisfies the pertinent
Federal guidance presented in Attachment C of Office of Management and Budget
Memorandum 03-09 *Reporting Instructions for the Federal Information Security
Management Act and Updated Guidance on Quarterly IT Security* Reporting issued
August 6, 2003."

We note that, as our program has matured, OIG evaluations have become more rigorous
as well. We appreciate that this increased level of evaluation will allow us to continue to
mature and improve our processes, and thus our IT security, beyond minimum
requirements. Please note that improvement of IT security beyond documented OMB or
NIST requirements may not be our highest priority for available critical IT security
funding. However, as we evaluate our overall IT security funding needs and available
resources, we will consider recommendations in light of priorities in the program.

We appreciated meeting with OIG staff and management early in this evaluation process.
These meetings provided us an opportunity to begin immediate implementation of
proposed recommendations. Our immediate action significantly improved our processes
during this fiscal year. We also appreciate that BOR, MMS, NBC, and BLM were
specifically noted for effective implementation of POA&M practices. These and other
practices served as the basis for improved guidance Department-wide.

25

DoI-OIG Annual I-T
Security Program Evaluation
Page 31 of 38   Defendants' Notice of Filing of
                                       DoI's FY 2005 FISMA Reports

Our responses to the recommendations are outlined below.

Recommendation 1:

Institute a quality assurance process to ensure:

b) *All weaknesses are reported.*

b) *Weaknesses are completely described and the respective corrective actions would adequately correct the weaknesses. This could be partially addressed through establishing standardized descriptions of common weaknesses and related corrective actions.*

Response:

a) Quality assurance programs are an important part of a maturing process. Based on OIG recommendation, the Department issued guidance requiring, "Each IT security weakness identified in any review of a program or system must be entered on the authoritative POA&M (e.g., all Notice of Findings and Recommendations (NFRs) from OIG audits, Security Test and Evaluation (ST&E) and risk assessment reports, NIST SP 800-26 self-assessments, internal/external penetration testing, vulnerability scanning, site/facility compliance reviews, C&A package compliance reviews, etc.)."

OMB guidance may not have kept pace with incident management requirements and vulnerability monitoring tools or capabilities often employed by Federal agencies. Incident management procedures at many Federal agencies require officials to employ immediate action to safeguard systems and data from outside threats or vulnerabilities. The management of such rapidly handled changes may be better addressed through other processes. Furthermore, it may not be prudent to disclose such vulnerability details in POA&Ms. The use of vulnerability monitoring tools should also be considered as an acceptable adjunct to the POA&M. Since these tools often provide misleading results or false-positives and other errors, the information needs to be screened before putting information in POA&Ms and should still be summarized.

b) We initiated a quality assurance process by OCIO Directive 2005-007, May 3, 2005, with which all bureaus complied. Copies of bureau and office verifications have been provided to your office. We used our experience with this initial process and the recommendations provided in your report to refine and clarify our procedures, as issued by memorandum of August 18, 2005. However, we plan to issue additional guidance in a new OCIO Directive and POA&M Process Standard for implementation in FY 2006 to further enhance POA&M processes. This additional guidance has been developed by a team of specialists from throughout the Department and will provide more recommended standardization.

OMB M-04-25 states that "*sensitive descriptions of the specific weakness are not necessary*" (p. 15) and endorses the use of general or brief descriptions. A template

2

attached to the OMB memorandum also provided examples on the type of descriptive information required on IT security weaknesses. The example illustrates that high-level descriptions of IT security weaknesses is acceptable. Separate source documents and reports detail more fully each finding described in the POA&M, and provides adequate traceability.

We believe the implementation of the existing quality assurance process fully implements this recommendation.

Recommendation 2:

Institute a verification process to ensure that weaknesses reported as corrected are, in fact, corrected; that supporting documentation is maintained; and that management's acceptance of risk is appropriately justified and documented.

Response:

We initiated a quality assurance and verification process by OCIO Directive 2005-007, May 3, 2005, with which all bureaus complied. Your office has been provided copies of bureau and office verifications that weaknesses that were reported as corrected were in fact corrected. We used our experience with this initial process and the recommendations provided in your report to refine and clarify our procedures, as issued by memorandum of August 18, 2005.

However, we also intend to issue a new OCIO Directive and POA&M Process Standard for implementation in FY 2006 to further enhance the POA&M process. This additional guidance has been developed by a team of specialists from throughout the Department and will provide much of the recommended standardization. The POA&M Process Standard will provide for an additional quality assurance process, to be performed by the OCIO, which will include inspection and review of a sample set of completed POA&M corrective actions each fiscal year.

The use of cost benefit analyses is recommended along with other factors to be considered when making such decisions. However, it is not cost effective for agencies to complete cost-benefit analyses for every security weakness that falls into the risk acceptance category.

We believe the implementation of the existing quality assurance and verification process fully implements this recommendation.

Recommendation 3:

Require senior bureau management to certify that information in the bureaus' POA&M is accurate and true.

3

Response:

The quality assurance and verification process initiated by OCIO Directive 2005-007, May 3, 2005, and further clarified by memorandum of August 18, 2005, requires senior management officials to ensure and verify information in the bureau's POA&M is accurate.

We believe the implementation of the verification process fully implements this recommendation.

Recommendation 4:

Institute a practice to review all Department IT system and program weaknesses to ensure the most critical weaknesses for the most critical systems of the Department are being addressed first.

Response:

Interior agrees with the spirit of this recommendation, but not the recommended corrective action, for the following reasons:

1. The Department receives its IT budget under the authority of multiple appropriations, and with specific restrictions on movement of appropriated funds among bureaus or programs. The recommendation for Department-wide prioritization of POA&M funding does not take into account the statutory restrictions, nor the practical implications of managing these investments. Interior's policy is clear that any risks determined critical or unacceptable must be fully funded for immediate mitigation and all risks above residual must be planned and funded within the Designated Approving Authority's (DAA) budget. Thus, prioritization across bureaus is not a relevant issue.

2. NIST SP 800-37 requires the DAA to make the final decision, and be held accountable, for accepting risks to their systems. If officials at other levels in the Department make changes to the DAA's determination, it would undermine both the DAA's authority and accountability. The DAAs and other senior management officials rely on a variety of factors in establishing scheduled commitments to correct weaknesses.

3. Interior's commitment to implement a planned corrective action to resolve known weaknesses as indicated in the "Scheduled Completion Date" column represents senior management's priority in addressing weaknesses. Both IATO status and/or planned dates for implementing corrective actions represent the DAA's degree of tolerance and duration for continued exposure to risks resulting from identified weaknesses.

4

4. Sequential prioritization based on risk level alone does not make sense in an operational and budgetary context where some weaknesses are more easily and quickly corrected than others. Adhering to a strictly sequential work-off plan could leave a larger number of weaknesses unresolved, which could increase the overall risks to individual systems, potentially raising the system risk to unacceptable levels.

5. Interior meets the OMB requirements, as risk levels and severity of weaknesses are identified in Risk Assessment reports and other source documentation. As described in DOI IRM Directive 2004-009 Appendix A, each bureau and office is required to establish a priority process for addressing IT system security weaknesses based on the significance of the vulnerability (See page C-4). Each system security weakness is assigned a priority level of High, Medium, or Low. The Department also established a requirement to address all high priority IT security weaknesses within 180-days. The Department's priority setting process, therefore, is adequate and fully complies with OMB guidance.

We believe no further action is needed to implement this recommendation.

Recommendation 5:

Improve the Department's automated POA&M system. To determine the best automated system for the Department, consult with bureaus' IT operational staff, system owners, program managers, and others that are involved with IT security weakness remediation. Also, canvass other Federal agencies that have implemented automated systems to manage POA&Ms.

Response:

Again, Interior agrees with the spirit of the recommendation, as automation improvements drive many enhancements to processes, and should be evaluated for efficacy. However, without such an evaluation, prescriptive improvements are premature. Nonetheless, Interior recognizes the benefits of using POA&M automation tools and plans to evaluate tools for prospective use in Interior, but may not be able to immediately implement the recommendation nor find it cost effective to do so.

As we evaluate possible automated solutions, please be aware that we must consider the following factors:

1. The current POA&M reporting format, while not optimal, meets basic program requirements. At this point, investing in a different POA&M tool may not be the highest priority for limited resources.

2. The Department has a structured process, with senior management level involvement and approval, for determining the need for automated tools and the priority for funding and implementing them. Also, as a new automated POA&M system was not included in the FY 2007 decisions, such a system could not be

5

29

Defendants' Notice of Filing of
DoI's FY 2005 FISMA Reports

funded until FY 2008. We are investigating opportunities for workflow improvement within approved IT security operations and maintenance funding.

3. Implementation of a single-purpose system for POA&Ms would be contrary to a standards-compliant, service-oriented, component-based architecture. Many of the functional requirements for security POA&Ms - such as forms automation, workflow automation, and document and records management - are common to other Departmental and OCIO processes, and those requirements should be met with common software service components. Likewise, some of the data required for POA&Ms must be shared with other applications, such as DEAR and eCPIC, and should be based upon a common data architecture that minimizes needless inconsistencies and redundancies, rather than potentially aggravating them through implementation of yet another stovepipe system. OCIO will be applying its Methodology for Business Transformation (MBT) to its own processes and the recommendations derived from the MBT should drive the establishment of priorities for sharing of data, retirement and/or consolidation of existing systems, and implementation of new capabilities. Through this process, we are also validating requirements with our bureaus, completing tool assessments and developing an investment proposal to be considered in the next capital planning cycle.

We believe we are compliant with OMB-specified POA&M reporting using the existing spreadsheet format, and therefore meet the requirements of this recommendation.

In summary, we believe we addressed all recommendations, eliminating any need to elevate concerns to the level of a material weakness for this fiscal year. We worked diligently to implement past and current OIG recommendations, and are committed to continued enhancements in our POA&M program. The assistance provided by OIG in identifying opportunities to strengthen the program was very valuable. Our current POA&M program meets OMB and NIST requirements, despite the many challenges in implementation this year, including staff turnover and unprecedented consumption of resources by the Department's largest civil case (*Cobell v. Norton*). Nonetheless, the Department's program continues to improve in maturity, awareness, accountability, integrity, efficiency, and quality assurance.

Recommendation and Implementation Status

Recommendation	Responsible Individual and Office	Status
1	W. Hord Tipton, Office of the CIO	completed
2	W. Hord Tipton, Office of the CIO	completed
3	W. Hord Tipton, Office of the CIO	completed
4	W. Hord Tipton, Office of the CIO	completed
5	W. Hord Tipton, Office of the CIO	completed

In general, this Evaluation Report is timely and provides constructive feedback for the POA&M program and process. We proactively incorporated the recommendations

6

presented here, such that they can now be considered fully implemented. I believe the POA&M process, following OMB direction, provides a sound program for managing the remediation of IT security weaknesses. I look forward to a continued positive relationship with your office as we further mature our IT security programs.

If you have any questions, please contact me at 202-208-6194. Staff may contact Mr. Larry Ruffin at 202-208-5419.

Attachments

1. OCIO Directive 2005-007, May 3, 2005
2. Memorandum of August 18, 2005
3. Draft POA&M Guidance

cc: Lynn Scarlett, AS/PMB

7

STATUS OF EVALUATION RECOMMENDATIONS

Recommendation	Status	Action Required
1, 2, 3, 4, and 5	Unresolved.	Reconsider the recommendation, and provide a corrective action plan that includes target dates and titles of officials responsible for implementation.

32