



Office of the Inspector General

Date April 20, 2007

To Cristián Samper, Acting Secretary

Cc Sheila P. Burke, Deputy Secretary and Chief Operating Officer  
Ann Speyer, Chief Information Officer  
Bruce Daniels, Director of IT Security and Smithsonian Computer Security Manager

From A. Sprightley Ryan, Inspector General

Subject Report on the Fiscal Year 2006 Federal Information Security Management Act (FISMA) Audit of the Smithsonian Institution's Information Security Program, Number A-06-05

Attached please find a copy of our final report on the FY 2006 FISMA audit of the Smithsonian Institution's Information Security Program. Our audit notes that OCIO made considerable progress to address the nine recommendations in our FY 2005 report to strengthen controls over inventory of major systems, the certification and accreditation process, and specialized IT security training. We have closed eight recommendations and continue to work with management to close the remaining open recommendation related to the tracking of specialized IT security training.

Nonetheless, our FY 2006 FISMA audit shows that significant work remains to ensure adequate controls are in place and operating effectively. We made 12 recommendations to strengthen controls over implementation of configuration baselines, security awareness and incident response training, and corrective action plans. Management generally concurred with 11 of the recommendations and non-concurred with 1 concerning major systems placed in production prior to being formally certified and accredited to operate. We continue to hold discussions with management to resolve our differences.

Please call me at 202-633-7050 if you have any questions.

**REPORT ON  
FY 2006 FISMA AUDIT OF THE  
SMITHSONIAN INSTITUTION'S  
INFORMATION SECURITY PROGRAM**

Cotton & Company LLP  
Auditors · Advisors  
635 Slaters Lane, 4<sup>th</sup> Floor  
Alexandria, Virginia 22314  
703.836.6701  
[www.cottoncpa.com](http://www.cottoncpa.com)

## CONTENTS

<b>Section</b>	<b>Page</b>
Purpose	1
Background	1
Objectives, Scope, and Methodology	2
Results:	3
1. Major System Operated Without Going Through Formal Certification and Accreditation Process	4
2. Standard Security Configuration Baselines Were Not Implemented	4
3. Incident Response Policies and Procedures Lack a Training Requirement	5
4. Security Awareness Training Procedures Were Not Being Followed	6
5. Controls Were Not Adequate to Ensure Annual Self Assessments Were Accurate and Complete	7
6. Standard Security Configuration Baselines Were Weak	9
7. Major System Security Plans Do Not Include Minimum Security Controls Section	10
8. Some Major System Plan of Action and Milestone Schedules Were Missing Pertinent Data	11
Status of Prior-Year Recommendations	12
Summary of Management Response	14
Office of the Inspector General Comments	15
Appendix A CIS Benchmark Comparison for Oracle 9i/10g	17
Appendix B CIS Benchmark Comparison for Windows 2003 Domain Controller	18
Appendix C Full Text of Management Response	19

**REPORT ON  
FY 2006 FISMA AUDIT OF THE  
SMITHSONIAN INSTITUTION'S  
INFORMATION SECURITY PROGRAM**

Cotton & Company LLP conducted an audit of the Smithsonian Institution's (Institution) security management program and practices in accordance with Title III of the 2002 E-Government Act, also known as the Federal Information Security Management Act (FISMA).

**PURPOSE**

The E-Government Act of 2002 (Pub. L. No. 107-347), which includes Title III, the Federal Information Security Management Act of 2002 was enacted to strengthen the security of federal government information systems. Although the E-Government Act of 2002 does not apply to the Institution, the Institution supports the information security practices required by the Act because they are consistent with and advance the Institution's mission and strategic goals.

FISMA outlines federal information security compliance criteria, including the requirement for an annual independent assessment by the Institution's Inspector General. This report presents the results of the Smithsonian Institution's Office of the Inspector General (OIG) annual evaluation of the information security controls implemented by the Institution, based primarily on the work performed by Cotton & Company LLP.

**BACKGROUND**

FISMA, Office of Management and Budget (OMB) regulations and National Institute of Standards and Technology (NIST) guidance outline minimum security requirements for federal information security programs. These include:

- **Annual System Self-Assessments.** NIST's *Security Self Assessment Guide for Information Technology Systems* contains specific control objectives and techniques against which a system can be tested and measured. Performing a self-assessment and mitigating any of the weaknesses found in the assessment is an effective way to determine if the system or the information it contains is adequately secured and protected from loss, misuse, unauthorized access, or modification. OMB guidelines require organizations to use the NIST self-assessment tool annually to evaluate each of their major systems.
- **Certification and Accreditation.** NIST's *Guide for the Security Certification and Accreditation of Federal Information Systems* states that systems should be certified and accredited. A certification is "a comprehensive assessment of management, operational and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly and operating as intended." NIST guidance also discusses systems accreditation, which is "the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to operations, assets, or individuals based on the implementation of the agreed-upon set of security controls." Organizations should use the results of the certification to reassess their risks and update system security plans to provide the basis for making security accreditation decisions.

- **System Security Plan.** NIST's *Guide for Developing Security Plans for Federal Information Systems* requires that all major application and general support systems be covered by a security plan. The plan provides an overview of the security requirements of a system and describes controls in place or planned for meeting those requirements. Additionally, the plan defines responsibilities and the expected behavior of all individuals accessing the system. The NIST guide also instructs that the security plan should describe the management, operational, and technical controls the organization has implemented to protect the system. Among other things, these controls include user identification and authentication procedures, contingency/disaster recovery planning, application software maintenance, data validation, and security awareness training.

#### OBJECTIVES, SCOPE, AND METHODOLOGY

On behalf of the OIG, Cotton & Company performed an independent audit of the Institution's information security management program. We conducted this audit in accordance with *Generally Accepted Government Auditing Standards*, 2003 Revision, as amended, promulgated by the Comptroller General of the United States. This report is intended to meet the objectives described below and should not be used for other purposes.

The objectives were to evaluate and report on the effectiveness of the Institution's information security program and practices by:

- Reviewing existing system security plans, policies, and procedures for compliance with applicable laws and regulations.
- Determining if mission-critical systems and interfaces across the Institution have been identified in the system inventory.
- Identifying new systems or systems significantly modified during the year and determining if they were certified and accredited.
- Determining if system categorizations comply with guidance identified in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- Reviewing major application and general support system self-assessments performed by system owners.
- Assessing the effectiveness of procedures for mitigating system deficiencies through the Plan of Action and Milestone (POA&M) process.
- Determining the completeness of disaster recovery plans, particularly for the Institution's general support system (SInet).
- Completing the OIG FISMA template in accordance with Section C of the OMB's Memorandum M-06-20, dated July 17, 2006.

To accomplish these objectives, we evaluated the Institution's security program, plans, policies, and procedures in place as of August 31, 2006, for compliance with applicable federal laws and regulations including specific guidance issued by OMB and NIST. Our audit included a high-level review of each of the Institution's 18 major systems and more detailed steps to evaluate the Institution's policies, procedures, and practices for:

- Certification and accreditation,
- POA&M,
- Security awareness training,
- Technical security training, and
- Incident response.

Additionally, we evaluated management actions completed through August 31, 2006, to address recommendations contained in the OIG's FY 2005 FISMA evaluation, Report No. M-05-03, issued February 16, 2006.

Our audit was based on detailed interviews with Office of the Chief Information Officer (OCIO) personnel and major system owners or sponsors. We reviewed policies, procedures, and practices for compliance with NIST and OMB guidance and, where possible, tested the Institution's policies, procedures, and controls for effectiveness.

## RESULTS

Our audit of the Institution's security management program and practices determined that while progress has been made in complying with requirements identified by FISMA, significant work is still necessary to ensure adequate controls are in place and operating effectively. The Institution made notable progress in addressing prior year weaknesses. Of the 9 recommendations in the OIG's FY2005 FISMA evaluation report, 7 were closed in FY2006 and 1 in December 2006. Specific areas where the Institution made progress include:

- Updating the Institution's system inventory to include system interfaces,
- Developing and testing disaster recovery plans,
- Establishing an interconnection agreement with the Smithsonian Astrophysical Observatory (SAO),
- Including completed items on the POA&Ms for one year after the completion date,
- Updating security plans based on changes to security configuration checklists, major system and operating environment changes, and the results of annual self-assessments,
- Completing self-assessments by mid-August 2006, and
- Certifying and accrediting systems affected by moving the data center to Herndon.

The one remaining recommendation concerning specialized IT security training has not been closed. Currently, project managers are the only personnel with completed plans. Training plans are being developed for network staff, IT project managers, and security staff. In addition, the Office of Human Resources (OHR) has developed a database that contains fields for recording course titles, hours, and completion dates; however, there is no implemented process or requirement for users to report training to OHR or OCIO for more formal tracking.

In addition, we noted that OCIO has thoroughly developed and documented IT policies and procedures. However, due to the Institution's decentralized IT environment, the implementation and enforcement of these policies and procedures has been limited or inconsistent. Without the centralization of IT operations and the assignment of responsibility within OCIO for ensuring Institution policy and procedures are being followed, management cannot ensure adequate

controls are in place. More control and oversight of IT operations should reside with OCIO, with the sole exception of the OIG, which must remain independent.

The following is a more detailed discussion of the weaknesses we found in our FY 2006 FISMA audit as well as 12 recommendations for strengthening management controls over the Institution's information security program. We present our findings in the order of greatest risk to the system.

### **Major System Operated Without Going Through Formal Certification and Accreditation Process**

Controls were not adequate to ensure that all the Institution's major applications have gone through a timely, formal certification and accreditation (C&A) process and received authorization for processing before being placed in production. Although OCIO has made significant progress in certifying and accrediting their major applications, we determined the C-Cure badging system (badging system) currently in production had not received official certification and accreditation to operate as of August 31, 2006. OCIO identified the badging system as a major application in the beginning of FY 2006 and stated that they were in the process of certifying and accrediting the system. We followed up with OCIO and determined the badging system received interim approval to operate on October 30, 2006 and full accreditation on November 16, 2006 after remediation of identified weaknesses.

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; B. *Descriptive Information*; b. *Controls for Major Applications*, (4) *Authorize Processing*, states:

...The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

The C&A process is intended to identify and mitigate system weaknesses to an acceptable level before placing it into production. Without going through the C&A process, individuals responsible for managing the badging system could not reasonably ensure that it and related data were not subject to unacceptable levels of risk.

### **Recommendation**

1. We recommend that the CIO develop and put in place Institution-wide controls to ensure that major applications are not placed into production before going through a formal certification and accreditation process and receiving formal authorization to operate.

### **Standard Security Configuration Baselines Were Not Implemented**

Controls are not adequate to ensure standard security configuration baselines have been implemented on major applications in accordance with Institution policy. Specifically, IT-960-TN16, *Baseline & Configuration Management of Application, Database, and Web Servers section I.*, states:

System owners must use established OCIO baseline build documents and obtain the appropriate approvals prior to installing or updating the operating system for application, database, and web servers to be placed on SInet.

Standard security configuration baselines (baseline build documents) document the recommended security settings which should be implemented on a platform such as Oracle or Windows. OCIO

developed and documented their standard security configuration baselines for system sponsors to implement; however, we determined these baselines have not been implemented for all major systems.

For example, our audit of the Development and Membership Information System (DMIS) major application noted that baselines for the Oracle database and Windows operating system have not been implemented. Management has identified this weakness in the DMIS POA&M; however target dates for implementing baselines are not until sometime in 2007.

In addition, our audit of the Institution's SInet Windows Domain Controller noted that the Institution's Windows 2003 baseline has not been implemented on the domain controller even though OCIO is responsible for implementing and maintaining this server. IT-960-TN16, states:

Any network or application server attaching to SInet will comply with the approved baseline configuration specified in this technical note... Deviations from the approved configurations will require a waiver from the Chief Information Officer.

IT-960-TN16 I., *Section 3 Responsibilities I. System Owners*, states:

System owners must use established OCIO baseline build documents and obtain the appropriate approvals prior to installing or updating the operating system for application, database, and web servers to be placed on SInet... Formally review their server configuration files twice a year; or when there are major changes requiring an update to this technical note (including its appendices) and individual system configuration documents.

Without adequate controls in place to ensure that configuration baselines are developed and put in place over the Institution's major information systems, the confidentiality, availability, or integrity of Institution systems and related data may be at greater risk than management is willing to accept.

### **Recommendation**

2. We recommend that the CIO establish procedures to ensure existing policies requiring the use of standard baselines are implemented and enforced.

### **Incident Response Policies and Procedures Lack a Training Requirement**

Controls were inadequate to ensure that personnel with significant incident response roles and responsibilities understood and were capable of carrying out the Institution's incident response policies and procedures. Specifically, we noted that none of the key incident response personnel within OCIO had received training on the Institution's documented incident response policy and procedures. Additionally, we noted that the Institution's incident response policy does not specifically require incident response training or annual refresher training for key personnel.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Section 3.7.2, *Characteristics, Educated Constituency*, states:

Users need to know about, accept, and trust the incident handling capability or it will not be used. Through training and awareness programs, users can become

knowledgeable about the existence of the capability and how to recognize and report incidents.

In addition, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems, IR-2, Incident Response Training*, states:

The organization trains personnel in their incident response roles and responsibilities with respect to the information system and provides refresher training at least annually.

Without periodic incident response training for key personnel, management cannot ensure that incidents will be handled according to the Institution's policy and not result in greater damage to the Institution's systems than would have occurred if personnel had been appropriately trained.

### **Recommendation**

3. We recommend that the CIO conduct incident response training for individuals with significant incident response roles and conduct periodic refresher training at least annually.

### **Security Awareness Training Procedures Were Not Being Followed**

Controls were not adequate to ensure employees completed security awareness training in accordance with Institution policy IT-930-02, *Security Controls Manual section 3.2.2.1 On-line training*, which states:

All employees, volunteers, interns, visiting scholars, and contractor personnel who use the Institution's computers and networks must complete computer security awareness training annually. Directors of each museum, research center, or office will ensure that new employees, volunteers, interns, visiting scholars and contractor personnel complete the course within 30 days after beginning work and that each user completes the online computer security awareness tutorial annually.

We identified 13 new network users who were granted network access between July 9 and 20, 2006. Of the 13, four did not complete online awareness training within the required 30-day period. In addition, we randomly selected 45 individuals after September 30<sup>th</sup> to determine whether they had completed annual security awareness training. Of the 45 individuals selected, we identified 3 who had not completed annual security awareness training.

Responsibility for ensuring that Institution personnel attend security awareness training is assigned at the unit, museum, research center, or office director level. Although OCIO reviews attendance at the end of the year to ensure individuals have completed training and sends reminders to each unit reminding them to take training, we noted that responsibility for ensuring new employees complete training within the required 30-day period has not been assigned to an individual within OCIO.

Additionally, we determined OCIO has not specifically defined consequences for non-compliance with the Institution's security awareness training policy. OCIO has withheld computer hardware purchase authority from units in the past; however, this type of penalty is not defined in their policy.

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, states that agencies must "...ensure that all individuals are trained in how to fulfill their security responsibilities before allowing them access to the system." In addition, NIST Special Publication (SP) 800-50, *Building an Information Security Awareness and Training Program* states:

Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing IT:

- Understand their roles and responsibilities related to the organization's mission;
- Understand the organization's IT security policy, procedures, and practices; and
- Have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible.

Further, NIST SP 800-50 states:

As cited in audit reports, periodicals, and conference presentations, it is generally understood by the IT security professional community that people are one of the weakest links in attempts to secure systems and networks. The "people-factor" not technology is key to providing an adequate and appropriate level of security. ... A robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

Security awareness training is the primary vehicle for communicating the agency's security policies, procedures, practices, and the expected behaviors of employees and contractors. Without effective security awareness training, management's ability to communicate the agency's security policies and procedures is minimized, and the risk of unauthorized activities taking place by employees or contractors can increase.

## Recommendations

We recommend that the CIO:

4. Develop, document, and implement procedures to enforce Institution policy requiring individuals to complete security awareness training within 30 days of being granted a SInet account and annually thereafter.
5. Identify, document, and enforce consequences of noncompliance (such as revoking access to SInet until training is completed) with the Institution's security awareness training policy.

## Controls Were Not Adequate to Ensure Annual Self-Assessments Were Accurate and Complete

Controls were not adequate to ensure that annual self-assessments were accurate, complete and in accordance with Institution policy for all major Institution systems. Specifically, we determined that a self-assessment was not completed for the Institution's badging system, which was

identified as a major application in early 2006. OCIO stated they (OCIO in conjunction with the system sponsor) were in the process of completing the initial certification and accreditation for the system and were therefore not requiring a self-assessment be completed by the system sponsor. As of August 2006, OCIO's certification and accreditation effort had not been completed. Further, our review of completed self assessments noted that none of the system sponsors produced or retained supporting documentation during their assessments.

IT-930-01, *AIS Security Planning, Section 6.2, Periodic Re-Analysis of AIS Security*, states "...Each system sponsor is required to annually complete a Self Certification review using NIST SP 800-26... The Computer Security Manager will review the Self Certification by July 30<sup>th</sup>."

NIST SP 800-26 section 3. *Questionnaire Structure* states:

After each question, there is a comment field and an initial field. The comment field can be used to note the reference to supporting documentation that is attached to the questionnaire or is obtainable for that question... Additionally, the section may reference supporting documentation on how the control objectives and techniques were tested and a summary of findings.

Additionally, our testing identified specific instances where responses documented on self-assessments were inaccurate. We noted the following issues:

- SInet 800-26, Section 4.1.3, indicated that rules of behavior have been established and signed by users and integrated within the system. We selected a random sample of 45 users to determine whether they had signed rules of behavior. Of the 45, management could only provide us with 5 signed copies. (See companion SInet Audit Report, Number A-06-07)
- SInet 800-26, Section 6.1.8, identified a process for requesting, establishing, issuing, and closing user accounts and noted that the self-assessment response indicated the control has been tested and integrated into the system. However, we selected a random sample of 45 SInet user accounts to test and identified the following:
  - Network accounts are not being promptly disabled or deleted after a period of inactivity. Out of 12,053 SInet active accounts, 3,359 (28%) have not been used in more than 180 days.
  - Network accounts are not being promptly deleted when users leave the Institution. We selected a random sample of 45 individuals who had recently resigned and noted that 16 of the 45 individuals were still identified as active on the network. (See Audit Report Number A-06-07)
- SInet 800-26, Section 15.1.6, indicated that passwords were changed at least every 90 days or earlier, and this control was tested and integrated into the system. In our SInet report (see Audit Report Number A-06-07), we noted that passwords were not being consistently changed within 90 days.
- Visitor Count Management System (VCMS) Section 6.1.8 indicates that procedures have been developed, implemented, tested, and integrated; however our review of the VCMS POA&M noted this control was also reported as a weakness.

We were informed during our audit that although OCIO offered a 2-day course (not mandatory) on completing the NIST SP 800-26 self-assessments, system sponsors did not attend this training. In addition, because self-assessments were not provided to OCIO until early in August, OCIO did not sufficiently review the assessments before providing them to the auditor.

Without adequate knowledge or guidance on how to accurately complete annual self-assessments, management cannot be sure that self-assessments are effectively providing assurance that new risks have not been introduced into the production environment that it would be unwilling to accept if identified.

### Recommendations

We recommend that the CIO:

6. Comply with Institution policy by reviewing annual self-assessments to ensure they are completed accurately and require system sponsors to produce and retain adequate documentation to support conclusions made.
7. Require system owners to attend training provided by OCIO on completing self assessments.

### Standard Security Configuration Baselines Were Weak

Although OCIO went through a detailed process to develop and document their standard security configuration baselines, we noted these baselines did not address many security configuration settings identified in industry-accepted security configuration baselines. OMB Memorandum M-06-20, *FY2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, Section 18*, identifies what are minimally acceptable system configuration requirements and where they may be located:

Security configuration checklists are now available for computer software widely used within the Federal Government. The checklists may be found on the NIST Computer Security Division website as well as the NSA System and Network Attack Center website. OMB expects agencies to use the published configurations or be prepared to justify why they are not doing so. Inspectors General should review such use.

Specifically, we compared the Institution's Windows 2003 and Oracle baselines to the Center for Internet Security's (CIS) respective baselines and noted specific areas the Institution's baselines did not address. (See Appendixes A and B for comparisons)

Through discussions with OCIO we determined the Institution developed their own baselines and removed configuration settings or controls which they determined did not need to be implemented or were not applicable to Institution systems. Because baselines should show management's risk-based consideration for all controls applicable to a platform such as Windows or Oracle, industry best practices are to include all security settings in a baseline and specifically document on the baseline the reason why certain controls were not implemented.

Without a comprehensive baseline for system sponsors to use in securing their system, management cannot be sure all necessary security settings have been adequately addressed or implemented.

**Recommendations**

We recommend that the CIO:

8. Consider adopting industry-accepted baselines, such as those offered by NIST, the National Security Agency (NSA), or CIS. If OCIO decides to use their own baselines, we recommend OCIO compare them to industry-accepted baselines and update them where necessary to ensure the Institution's baselines address all known configuration options.
9. Update Institution policy and procedures to require system sponsors to document on implemented baselines those controls which management has chosen not to implement for valid business reasons.

**Major System Security Plans Do Not Include Minimum Security Controls Section**

Controls were inadequate to ensure that the Institution's major system security plans included information required by Institution, OMB, and NIST guidance. The Institution's IT-930-01, Section 2, *Concept and Requirements Definition Phase*, states:

The Project Manager prepares the AIS Security Plan, which is the repository for all security-planning documents generated during the life cycle.

OCIO has a standard template documented in IT-930-01, Appendix B, for project managers to use when developing system security plans. This security plan template includes 13 sections. We noted two of the Institution's system security plans [National Air and Space Museum (NASM) and National Museum of American History Multi MIMSY Collection Information System (MIMSY CIS)] did not include the minimum security controls section. Without inclusion of the minimum security controls in the security plan, specific control areas required by OMB A-130, Appendix III, were not addressed. The OMB A-130 controls not addressed included:

- Rules of Behavior
- Specialized Training
- Personal Security
- Incident Response Capability
- Contingency Planning
- Technical Security
- Public Access Controls

In addition, our review of the DMIS security plan noted that minimum security controls were documented although these controls were not included in or referenced to in the system security plan (see companion DMIS Audit Report Number A-06-08). NIST SP 800-18 *Guide for Developing Security Plans for Federal Information Systems* section 1.4 states:

The purpose of system security plans is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements.

Without inclusion of or reference to all documented controls in the system security plan, the risk of security policies and procedures not being followed or in place and operating effectively increases.

A lack of adequate controls in place to verify that security plans are being developed, documented, and approved in accordance with Institution, OMB, and NIST policy also increases the risk that controls over major systems have been inadequately identified and tested.

### Recommendation

10. We recommend that the CIO require system sponsors to update system security plans for NASM and MIMSY CIS to comply with IT-930-01 guidance.

### Some Major System Plan of Action and Milestone Schedules are Missing Pertinent Data

OMB Circular A-11 Part 7 states:

As defined in OMB Memorandum 02-01, a plan of action and milestones (POA&M), also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

The Institution has developed and implemented a POA&M process. POA&Ms are consistently developed for each of the Institution's major applications and sent to the CIO for inclusion in the Institution-wide POA&M. However, our review of completed POA&Ms for major systems noted that many are missing information required by IT-930-01, *Automated Information System (AIS) Security Planning Technical Standard & Guidelines* and OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*. Specifically, we noted the following issues with the Institution's major system POA&Ms:

- Financial Management System (FMS), Travel Management System (TMS), and Visitor Count Management System (VCMS) - Scheduled completion date for each milestone was not identified.
- SInet and Smithsonian Astrophysical Observatory Scientific Computing System (SAO) - Scheduled Completion Date states "TBD", and there is no 'Status' column.
- Art Collection Information System (ARTCIS) – There is no column for "Status."

Without adequate controls to ensure required information is included in the POA&M, management's ability to track and effectively mitigate known weaknesses in a timely manner is diminished.

### Recommendations

We recommend that the CIO:

11. Require system sponsors for the ARTCIS, SAO, VCMS, and SInet systems to update their POA&Ms to include all information required by IT-930-01.
12. Periodically review POA&Ms to ensure that they meet criteria identified in IT-930-01 and OMB Memorandum M-02-01.

Status of Prior-Year Findings and Recommendations (FY 2005 FISMA evaluation, Report No. M-05-03)

Prior Year Finding	Recommendation	Status
System Inventory Does Not Identify All of the Institution’s Mission-Critical System Interfaces	We recommend the CIO identify and include all system interfaces, including those that transfer sensitive data, in its major system inventory to comply with FISMA reporting requirements.	Closed 3/23/2006
Certification and Accreditation Process Needs Improvement - Security Plans for the 14 Major Systems Were Not Updated	We recommend that the CIO require units to update system security plans based on changes to security configuration checklists, major system and operating environment changes, and the results of annual self-assessments.	Closed 6/6/2006
Certification and Accreditation Process Needs Improvement – Systems are Operating without Finalized Disaster Recovery Plans	We recommend that the CIO develop a separate disaster recovery plan for the National Postal Museum’s collection information system and finalize the draft disaster recovery plans for the six major applications discussed in this report.	Closed 3/23/2006
Certification and Accreditation Process Needs Improvement – SAO Operates on a Non-Smithsonian System Without an Interconnection Agreement.	We recommend that the CIO work with Harvard University and SAO to establish an interconnection agreement between the Smithsonian and Harvard University for the SAO Scientific Computing System as required by NIST’s “ <i>Security Guide for Interconnecting Information Technology Systems</i> ”.	Closed 6/14/2006
Certification and Accreditation Process Needs Improvement – Significant System Changes Occurred with No Reaccreditation.	We recommend that the CIO ensure that the general support system and affected major applications are reaccredited after the primary data center and general support system are relocated to Herndon, Virginia, and establish a process for ensuring that all major systems are reaccredited when significant changes occur in systems and/or their operating environment, in accordance with NIST guidance.	Closed 9/29/2006

<p>Specialized IT Security Training Not Provided to All Employees with Significant Computer Security Responsibilities.</p>	<p>We recommend that the CIO require that employees who have significant computer responsibilities report their plans for meeting the specialized training requirements at the beginning of the fiscal year, and monitor employee progress during the year to ensure that training is completed.</p>	<p>Open                      Target 01/31/2007                      Training plans have not been created for all personnel. Currently, curriculums are being developed for network staff, IT project managers, and security staff. Project managers are the only personnel with completed plans.</p>
<p>Specialized IT Security Training Not Provided to All Employees with Significant Computer Security Responsibilities. (Continued)</p>	<p>We recommend that the CIO ensure, either through OCIO's current tracking process or the Human Resources Management System, that in FY 2006 individuals identify course titles, hours, and completion dates of specialized IT training to provide assurance that NIST training requirements are satisfied.</p>	<p>Closed                      12/21/2006</p>
<p>Improvements Needed to Facilitate the Annual FISMA Evaluation Process – Completed Action Plan Items Need to be Retained for a Minimum of One Year.</p>	<p>We recommend the CIO keep completed items in the action plan for one year after they have been fully mitigated.</p>	<p>Closed                      3/23/2006</p>
<p>Improvements Needed to Facilitate the Annual FISMA Evaluation Process – Self-Assessments.</p>	<p>We recommend that the CIO ensure self-assessments are completed and available no later than July 30, of each year.</p>	<p>Closed                      9/29/2006</p>

**Summary of Management Response**

Management's March 27, 2007, response to our draft report generally concurred with 11 of our 12 recommendations to strengthen the effectiveness of the Institution's information security program and practices. OCIO agreed that work remains to be done but indicates that efforts to further improve IT security are complicated by limited resources as well as changing OMB and NIST guidance. OCIO stated that successful completion of some of the recommendations will require resources not currently budgeted for in OCIO. Management disagreed with our recommendation to ensure that major applications were certified and accredited before being placed into production and receiving a formal authorization to operate because it maintains that it already has adequate safeguards in place.

Management's planned actions are summarized below:

**Recommendation 1.** Non-concur. OCIO believes that adequate controls are in place to ensure that major applications are not placed into production before going through a certification and accreditation (C&A) process. All Major Applications are required to participate in the Technical Review Board (TRB) process and as part of this process C&A is required.

**Recommendation 2.** Concur. OCIO will draft procedures by September 30, 2007 to ensure existing policies requiring the use of standard baselines are implemented and enforced.

**Recommendation 3.** Concur. OCIO indicates that this training was conducted on September 18, 2006, where key incident response staff were involved in running several incident response scenarios.

**Recommendation 4.** Concur. OCIO will draft and implement procedures by July 31, 2007 to enforce Institution policy requiring individuals to complete security awareness training within 30 days of being granted an SI network account.

**Recommendation 5.** Concur. OCIO will modify the Institution's policy to include consequences for noncompliance to the annual requirement for security awareness training by July 31, 2007.

**Recommendation 6.** Concur. By July 31, 2007, OCIO plans to rescind its policy requiring self-assessments, which will no longer be required by NIST. Instead, NIST will require annual assessments of selected controls in accordance with SP 800-53a, and OCIO has agreed to comply with the NIST guidance.

**Recommendation 7.** Concur. OCIO has chosen to withdraw the requirement for annual self-assessments under NIST SP 800-26. According to NIST guidance, SP 800-26 is to be replaced by SP 800-53a, which will require annual assessments of selected controls. Therefore, OCIO believes that training on completing self assessments would not be required.

**Recommendation 8.** Partial concurrence. OCIO agreed to review its baselines and compare them to newer industry accepted baselines, identify deviations, and document the differences by September 30, 2007. OCIO also agreed to review its baseline annually.

**Recommendation 9.** Concur. The CIO agreed to update Institution policy and procedures to require that system sponsors document on baselines those controls that management chose not to implement by July 31, 2007.

**Recommendation 10.** Concur. OCIO will update security plans during the 2007 recertification and reaccreditation process to ensure that minimum security controls are in place in accordance with the current version of IT 930-01.

**Recommendation 11.** Concur. OCIO stated that POA&M's have been updated to include all information required by IT-930-01.

**Recommendation 12.** Concur. OCIO stated that all POA&Ms have been updated to include scheduled completion date and status. OCIO will ensure in periodic reviews, and no less than annually, that the POA&Ms meet relevant criteria.

The full text of management's response is included in Appendix C.

### **Office of the Inspector General Comments**

Management's planned actions for recommendations 2 through 5, and 8 through 12, respond to the intent of our recommendations and we consider them resolved. Regarding planned actions for recommendations 6 and 7 on self-assessments, we note that while NIST SP 800-26 will likely be rescinded, there will be a replacement for it in SP 800-53a that requires annual assessments be conducted on selected controls. Therefore, the CIO needs to ensure that the annual assessments are accurate, complete, and properly supported as well as that individuals involved in conducting assessments are properly trained. With the understanding and expectation that OCIO will fully implement the anticipated guidance on annual assessments, we consider recommendations 6 and 7 resolved.

In evaluating management's response to this report, we held several discussions with the IT Security Director in an effort to clarify and resolve areas of disagreement. The only recommendation we could not ultimately reach resolution on is recommendation 1 on ensuring major applications are not placed into production before going through a formal C&A process. We agree with OCIO that once a system is identified as "major," the process of going through the Technical Review Board and certifying and accrediting the system before production is a sound one. However, the primary criterion for identifying systems as major was whether it was listed on an OMB Exhibit 300. As a consequence, OCIO did not certify and accredit smaller, less expensive, but in our view not necessarily less important systems such as Badging, VCMS, and DMIS. Recently, because these systems have either been upgraded or the data was subsequently recognized as sensitive they were re-categorized as major and OCIO has subjected them to the certification and accreditation process.

We are concerned that the Institution relies on other IT systems that contain sensitive, mission-critical data at the unit level but that have not been placed through the rigors of a certification and accreditation process because these smaller system applications have not required expenditures that would require them to be listed on an Exhibit 300. For example, there are systems at the National Zoological Park such as the Animal Records Keeping System, Medical Animal Records System, and the Single Population Animal Records Keeping System, that were never identified as major systems, yet we believe the information contained in these systems is mission-critical to the Zoo and the health and welfare of the animals. Also, the Office of Protection Services operates the NACIS database application system, which is critical for documenting and tracking the status of employee and contractor background investigations and suitability determinations. This important system has known weaknesses and is difficult to support. In our view, the methodology OCIO uses to identify major systems does not sufficiently consider risk or magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in

these smaller IT applications. The new CIO has an opportunity to reexamine the inventory of the Institution's IT systems and determine whether other smaller applications should be placed through a certification and accreditation process because they process sensitive data related to security, personnel, safety, or health. We will continue to hold discussions with OCIO to work toward a resolution on this issue.

We appreciate the courtesy and cooperation of Smithsonian representatives during this evaluation. If you have any questions concerning this report, please call me, or Stuart Metzger at (202) 633-7050.

**Appendix A**

*Appendix A documents our comparison of the Institution’s Oracle 9i/10g baseline to an industry-accepted Oracle baseline. Where the Institution’s baseline does not address controls in the industry-accepted baseline we noted a deficiency.*

*Note – The controls columns identify how many controls each baseline addresses in each focus area.*

CIS Benchmark for Oracle 9i/10g Ver 2.0			Smithsonian OCIO: Security Settings for Oracle Servers	
#	Area of Focus	Controls	Deficiencies	Controls
1	Operating System (OS) Settings	20	Only covers a few settings at the OS level, missing the majority of OS controls or a reference to an OS baseline.	3
2	Installation and Patch	14	Only covers a few settings regarding installation and patch management.	4
3	Oracle Directory and File Permissions	31	Does not cover OS level permissions in detail and does not cover modifications to key files init.ora, listener.ora, and sqlnet.ora.	0
4	Oracle Parameter Settings	31	Substantially not covered.	1
5	Encryption Settings	24	Substantially not covered.	1
6	Startup and Shutdown	3	Not covered.	0
7	Backup and Recovery	8	Generic statement concerning the creation of backup procedures, nothing specific.	3
8	Oracle Profile – Setup Settings	14	Generic statement covering profile settings, specifics not identified.	1
9	Oracle Profile – Access Settings	59	Some permission restrictions are covered, but not to the extent in CIS.	13
10	Enterprise Manager	6	Not covered.	0
11	10g Specific Settings	4	Not Applicable for DMIS	0
12	General Policy and Procedures	63	Some general database admin procedures covered.	11
13	Audit Policy and Procedures	23	Not covered.	0
14	Appendix A – Additional Settings	14	Not covered.	0
		N/A	Other controls not specifically covered by CIS	6

**Appendix B**

*Appendix B documents our comparison of the Institution’s Windows 2003 baseline to an industry-accepted Windows 2003 baseline. Where the Institution’s baseline does not address controls in the industry-accepted baseline we noted a deficiency.*

*Note – The controls columns identify how many controls each baseline addresses in each focus area.*

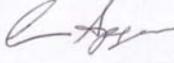
<b>CIS Benchmark for Windows 2003 Domain Controller</b> (Control totals reflect all listed settings, even the ones where a setting is not specified. These will automatically pass unless the target baseline implements an insecure setting)			<b>Smithsonian OCIO: Security Settings for Windows 2003 baseline</b>	
#	Area of Focus	Controls	Deficiencies	Controls
1	Service Packs and Hotfix Requirements	2	No deficiencies, the document describes how to update the machine upon setup.	2
2	Audit Policy	9	Auditing Object Access is not defined.	8
3	Account Policy	6	The minimum password age is set to 0 instead of 1.	5
4	Account Lockout Policy	3	No deficiencies.	3
5	Event Log Settings	12	No deficiencies.	12
6	Security Settings	87	Several of the security settings were not defined, when they should have specific values defined.	59
7	Services	39	Several services were not defined, specifically, defining dangerous services to be disabled.	2
8	User Rights	39	Several user rights were not specifically defined. One of the defined user rights had inappropriate rights given to the Users group for “Allow logon through terminal services.”	21
9	File Permissions	27	Not covered.	0
10	Registry Permissions	11	Not covered.	0
11	File and Registry Auditing	3	Not covered (cannot be done without Auditing Object Access).	0

Appendix C Management Response



Smithsonian Institution  
Office of the Chief Information Officer

---

**Date:** March 27, 2007  
**To:** A. Sprightley Ryan, Inspector General  
**cc:** Bruce Daniels, Smithsonian Computer Security Manager  
**From:** Ann Speyer, Chief Information Officer   
**Subject:** OCIO Response To the OIG Draft Audit Report on the FY 2006 FISMA Audit of the Smithsonian Institution's Information Security Program, Number A-06-05, dated February 20, 2007

OCIO is pleased to provide it's response to the OIG Draft Audit Report on the Fiscal Year 2006 Federal Information Security Management Act (FISMA) Audit of the Smithsonian Institution's Information Security Program, Number A-06-05, dated February 20, 2007.

In the attached report, each issue presented in the audit report is addressed in order. Please contact me at 202-633-1688 or Bruce Daniels, Smithsonian Computer Security Manager, at 202-633-6000, if you have any questions.

Appendix C Management Response (continued)

**OCIO Response:**  
*OIG Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

**TABLE OF CONTENTS**

Table of Contents ..... 3  
 Background ..... 3  
 General Comments ..... 3  
 Report Items and OCIO Responses ..... 4

**BACKGROUND**

In FY 2006 Cotton & Company LLP conducted an audit of the Smithsonian Institution's security management program and practices for the SI Inspector General in accordance with the E-Government and Federal Security Management (FISMA) Acts of 2002. A discussion draft of the report of the results of the audit was presented to the Smithsonian's acting Chief Information Officer, Ann Speyer, and Computer Security Manager, Bruce Daniels, by Joan Mockridge of the Office of the Inspector General and an exit conference was held on January 19, 2007. An updated draft report, dated February 20, 2007 was delivered to the CIO. This document contains the Office of the Chief Information Officer's response to the February 20, 2007 draft report.

**GENERAL COMMENTS**

OCIO agrees that work remains to be done to completely secure the Smithsonian IT environment. However, significant improvements have been made in SI's security posture over the past three years. Efforts to further improve security are complicated by limited resources as well as changing OMB and NIST guidance. OCIO continues to appreciate input from the Inspector General's office.

Successful completion of some of the recommendations, including recommendations 2, 8, and 9 will require resources that have not currently been budgeted in OCIO.

380 Herndon Parkway  
 MRC 1010  
 Herndon VA 20170

ocioResponse\_IIGReportOnFY2006FISMAAudit\_03-27-2007.doc  
 Page 3 of 9

Appendix C Management Response (continued)

**OCIO Response:**  
*OIG Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

**AUDIT RECOMMENDATIONS AND OCIO RESPONSES**

Page	Recommendation	OCIO Response	Target Dates
4	<p>Recommendation 1: We recommend that the CIO develop and put in place Institution-wide controls to ensure that major applications are not placed into production before going through a formal certification and accreditation process and receiving formal authorization to operate.</p>	<p>Non-Concur: OCIO believes that adequate controls are in place to ensure that major applications are not placed into production before going through a certification and accreditation (C&amp;A) process. All Major Applications are required to participate in the Technical Review Board (TRB) process. As part of this process C&amp;A is required.</p> <p>Smithsonian Directive 920 establishes life cycle management (LCM) policies, defines essential elements, and assigns responsibilities governing the initiation, definition, design, development, deployment, operation, maintenance, enhancement, and retirement of automated information systems (AIS) and IT infrastructure projects at the Smithsonian Institution.</p>	N/A
		<p>The badging system initially did not fall in the categorization of a major system. New work on the system, specifically revolving around HSPD 12, caused a review of the system and subsequently resulted in the re-categorization of the system as a major application.</p>	

380 Herndon Parkway  
MRC 1010  
Herndon VA 20170

ocioResponse\_JGReportOnFY2006FISMAAudit\_03-27-2007.doc  
Page 4 of 9

Appendix C Management Response (continued)

**OCIO Response:**  
*OIG Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

<p>5                  Recommendation 2:                  We recommend the CIO establish procedures to ensure existing policies requiring the use of standard baselines are implemented and enforced.</p>	<p>Concur                  OCIO will draft procedures to ensure existing policies requiring the use of standard baselines are implemented and enforced.</p>	<p>09/30/07</p>
<p>6                  Recommendation 3:                  We recommend that the CIO conduct incident response training for individuals with significant incident response roles and conduct periodic refresher training at least annually.</p>	<p>Concur:                  OCIO is already conducting this training per SI's incident response policy which contains this requirement. See IT 930-02, page 60, section 3.8.2. Primary SI incident responders undertook Annual Incident response training on September 18, 2006. During this training, key incident response staff were involved in running several incident response scenarios.</p>	<p>Completed                  09/18/06</p>
<p>7                  Recommendation 4:                  We recommend that the CIO develop, document, and implement procedures to enforce Institution policy requiring individuals to complete security awareness training within 30 days of being granted a SInet account and annually thereafter.</p>	<p>Concur:                  OCIO will draft and implement procedures to enforce Institution policy requiring individuals to complete security awareness training within 30 days of being granted an SI network account. Procedures for tracking users annually thereafter are already in place.</p>	<p>07/31/07</p>
<p>7                  Recommendation 5:                  We recommend that the CIO identify, document and enforce consequences of noncompliance (such as revoking access to SInet until training is completed) with the Institution's security awareness training policy.</p>	<p>Concur:                  OCIO will draft procedures for enforcing the security awareness training and will modify the Institution's policy to include consequences for noncompliance.</p>	<p>07/31/07</p>

380 Herndon Parkway  
 MERC 1010  
 Herndon VA 20170

ocioResponse\_IIGReportOnFY2006FISMAAudit\_03-27-2007.doc  
 Page 5 of 9

Appendix C Management Response (continued)

**OCIO Response:**  
*OIG Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

9	<p>Recommendation 6: We recommend that the CIO comply with Institution policy by reviewing annual self-assessments to ensure they are completed accurately and require system sponsors to produce and retain adequate documentation to support conclusions made.</p>	<p>Concur: OCIO will change policy so that self assessments are no longer required. This is in agreement with NIST policy as we understand it. Annual assessments of selected controls based on the SP 800-53 controls will be undertaken</p>	07/31/07
9	<p>Recommendation 7: We recommend that the CIO require system owners to attend training provided by OCIO on completing self assessments.</p>	<p>Concur: FY 2006 is the last year that annual self assessments will be used at the Smithsonian Institution. OCIO will change policy so that self assessments are no longer required. This is in agreement with NIST policy as we understand it. Annual assessments of selected based on the SP 800-53 controls will be undertaken Training on completing self assessments would not be required.</p>	07/31/07
9	<p>Recommendation 8: We recommend that the CIO consider adopting industry-accepted baselines such as those offered by NIST, National Security Agency (NSA), or CIS.</p>	<p>Partial Concur, and agree to review baselines annually. The Smithsonian baseline was derived from an industry</p>	9/30/07

380 Herndon Parkway  
MRC 1010  
Herndon VA 20170

ocioResponse\_IIGReportOnFY2006FISMAAudit\_03-27-2007.doc  
Page 6 of 9

Appendix C Management Response (continued)

**OCIO Response:**  
*OCIO Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

<p>If OCIO decides to use their own baselines, we recommend OCIO compare them to industry accepted baselines and update them where necessary to ensure the Institution's baselines address all known configuration options.</p>	<p>standard. SI adopted its standard based on the <i>Microsoft Solutions for Security Windows Server 2003 Security Guide and associated Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP</i> which provides a comprehensive look at all of the major security settings present in Windows Server 2003 and XP. The Smithsonian identified its target enterprise security environment as matching that of the "Enterprise Client" level defined in the guides, using the Microsoft Enterprise Client security templates as a starting point for hardening the OS. Additional lockdowns were then added based on analysis of SI's environment. SI did not "remove configuration settings or controls which they determined did not need to be implemented or were not applicable to Institution systems." Upon completion of the baseline, SI hired a nationally recognized security firm to perform IV&amp;V penetration testing on the baseline. The baseline and penetration testing results were then presented to the OIG at their offices in the Victor Building. OCIO feels that this baseline represents best practices and has proven this through independent evaluation and in-the-field usage. SI used all available models when it developed it's baseline. NIST had not yet published theirs at this time. However, it is likely that SI's is quite similar as there is a common body of knowledge regarding the appropriate settings and this common body of knowledge was used. The baseline build is well</p>
---	---

380 Herndon Parkway  
 MRC 1010  
 Herndon VA 20170

Appendix C Management Response (continued)

**OCIO Response:**  
*OIG Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

	<p>documented and referenced.</p> <p>The auditors did not review the Smithsonian baseline as it compares to the Microsoft baseline we adopted.</p> <p>OCIO agrees to review baselines to see where deviations exist between OCIO baseline and newer industry accepted baseline. OCIO will document differences between adopted baseline and industry accepted baseline.</p>	
<p>9</p> <p>Recommendation 9:                  We recommend that the CIO update Institution policy and procedures to require system sponsors to document on implemented baselines those controls which management has chosen not to implement for a valid business reason.</p>	<p>Concur</p> <p>CIO will update Institution policy and procedures to require system sponsors to document on implemented baselines those controls which management has chosen not to implement for a valid business reason.</p>	<p>07/31/07</p>
<p>10</p> <p>Recommendation 10:                  We recommend that the CIO require system sponsors to update system security plans for NASM and NMAHCIS to comply with IT-930-01 guidance.</p>	<p>Concur:</p> <p>NASM and NMAH CIS were accredited under an earlier version of 930-01 in which the minimum security control requirement did not exist. Both systems were fully compliant with IT 930-01. The Security Plans for these systems did list security controls. These applications were accredited for a three year period.</p> <p>OCIO has changed policy documentation so that systems accredited under an earlier version of the IT 930-01 will be grandfathered for that version and not</p>	<p>Completed                  3/27/07</p>

380 Herndon Parkway  
 MRC 1010  
 Herndon VA 20170

ocioResponse\_IIGReportOnFY2006FISMAAudit\_03-27-2007.doc  
 Page 8 of 9

Appendix C Management Response (continued)

**OCIO Response:**  
*OIG Report On FY 2006 FISMA Audit Of The Smithsonian Institution's Information Security Program*

	<p>required to meet existing documented standards until a recertification and reaccreditation is completed</p> <p>When they submit for re-accreditation in 2007 OCIO will review their submission to assure that the minimum controls are documented as per the current version of IT-930-01.</p>	
<p>11 Recommendation 11:                  We recommend that the CIO require system sponsors for the ARTCIS, SAO, VCMS, and SInet systems to update their POA&amp;Ms to include all information required by IT-930-01.</p>	<p>Concur:                  These POA&amp;M have already been modified to reflect the required information</p>	<p>Completed                  01/31/07</p>
<p>11 Recommendation 12:                  We recommend that the CIO periodically review POA&amp;Ms to ensure that they meet criteria identified in IT-930-01 and OMB Memorandum M-02-01</p>	<p>Concur:                  OCIO periodically reviews POA&amp;Ms at least annually. Part of the review process is to ensure that they meet criteria identified in IT-930-01 and OMB Memorandum M-02-01. However, in some instances the individuals who create the POA&amp;M are not the individuals with direct resource responsibility. For this reason, several POA&amp;Ms did not have scheduled completion dates. All POA&amp;Ms have been updated to include scheduled completion date and status.</p>	<p>Completed                  01/31/07</p>

380 Herndon Parkway  
 MRC 1010  
 Herndon VA 20170

ocioResponse\_JGReportOnFY2006FISMAAudit\_03-27-2007.doc  
 Page 9 of 9