



# Smithsonian Institution

Office of the Inspector General

Date February 16, 2006

To Lawrence M. Small, Secretary  
Sheila P. Burke, Deputy Secretary and Chief Operating Officer

cc John E. Huerta, General Counsel  
Dennis R. Shaw, Chief Information Officer

From *Debra S. Ritt*  
Debra S. Ritt, Inspector General

Subject Independent Evaluation of Smithsonian Institution Information Security Practices

Attached is our report on the evaluation of the Institution's information security program for FY 2005. The evaluation was performed by Richard S. Carson & Associates, Inc. and was supplemented with an OIG review of additional documentation provided by the Office of the Chief Information Officer through January 2006.

We determined that OCIO has established a comprehensive framework for ensuring the security of federal information systems within the Smithsonian Institution. While the framework established by OCIO addresses all of the critical components needed to protect the Institution's federal information system assets, our evaluation identified the following areas where implementation of the Institution's security program could be improved; inventory of major systems, certification and accreditation process, and specialized IT security training. Additionally, we identified that improvements were needed in OCIO's reporting practices to better facilitate our annual evaluation of the Institution's security program.

Management generally agreed with the report findings and conclusions related to its major system inventory, tracking of specialized IT security awareness training, and improvements needed in the timing of annual self-assessments. However, management disagreed with deficiencies we noted in its certification and accreditation process and the need to retain (for 1 year) mitigated IT security weaknesses on its Plan of Action and Milestones Report.

Despite these disagreements, management believes the report's recommendations will strengthen the Institution's security accreditation process for major IT systems. The CIO generally concurred with eight of our recommendations and non-concurred with another. We considered management's planned actions responsive to all but one of our recommendations. However, we will consider the non-concurrence as an unresolved recommendation until we obtain clarification from OMB on its FISMA reporting instructions.

## Attachment

Victor Building Suite 4200  
750 Ninth Street NW  
Washington DC 20560-0905  
202.275.2244 Telephone  
202.275.1435 Fax



# Smithsonian Institution

**Office of the Inspector General**

**Review of Smithsonian Institution  
Information Security Practices**

**OIG Report Number M-05-03**

**February 16, 2006**

---

---

## TABLE OF CONTENTS

<b>INTRODUCTION .....</b>	<b>1</b>
PURPOSE.....	1
BACKGROUND .....	1
OBJECTIVES, SCOPE, AND METHODOLOGY.....	2
<b>RESULTS.....</b>	<b>3</b>
SYSTEM INVENTORY DOES NOT IDENTIFY ALL OF THE INSTITUTION'S MISSION-CRITICAL SYSTEM INTERFACES.....	4
CERTIFICATION AND ACCREDITATION PROCESS NEEDS IMPROVEMENT.....	5
SPECIALIZED IT SECURITY TRAINING NOT PROVIDED TO ALL EMPLOYEES WITH SIGNIFICANT COMPUTER SECURITY RESPONSIBILITIES.....	9
IMPROVEMENTS NEEDED TO FACILITATE THE ANNUAL FISMA EVALUATION PROCESS.....	10
<b>MANAGEMENT COMMENTS .....</b>	<b>11</b>
<b>OFFICE OF THE INSPECTOR GENERAL RESPONSE.....</b>	<b>12</b>
<b>APPENDIX.....</b>	<b>14</b>

## INTRODUCTION

### PURPOSE

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

### 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*<sup>1</sup> 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*<sup>2</sup> 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 system accreditation, which is "the official management decision 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.

---

<sup>1</sup> NIST Special Publication 800-26, November 2001.

<sup>2</sup> NIST Special Publication 800-37, May 2004.

- **System Security Plan.** NIST's *Guide for Developing Security Plans for Information Technology Systems*<sup>3</sup> requires that all major applications 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

Richard S. Carson & Associates, Inc., on behalf of the OIG, performed an independent evaluation of the Institution's information security program.

The purpose of the independent evaluation was to assist the OIG in meeting its FISMA obligation for an independent assessment of the Institution's information security program in accordance with OMB Fiscal Year (FY) 2005 reporting guidelines. The objectives of the independent evaluation were to:

- Determine the effectiveness of Institution information security policies, procedures, and practices.
- Review the network/system security of a representative subset of the Institution's major application and general support systems.
- Assess the Institution's compliance with FISMA and related OMB and NIST information security policies, procedures, standards, and guidelines.
- Assess the Institution's progress in correcting weaknesses identified in the FY 2004 Plan of Action and Milestones (action plan).

In support of these objectives, the evaluation team conducted a qualitative review of the Institution's information security program, specifically evaluating the degree of compliance with applicable OMB and NIST criteria for a security program and evaluating the effectiveness of automated and manual security controls for the Institution's general support and mission-essential systems. The evaluation included a cursory review of all 14 systems and a more comprehensive review of two systems:

- Smithsonian Institution Network Infrastructure, General Support System, and
- Smithsonian Institution Research Information System (SIRIS), Major Application.

The team's evaluation was based on interviews with Office of the Chief Information Officer (OCIO) staff, prior OIG reports of Institution systems, and a document review to assess compliance with OMB and NIST guidance.

The evaluation was conducted at the Smithsonian's OCIO Security Operations Division between August 17, 2005 and September 30, 2005, and was supplemented with a review of additional documentation provided by OCIO through January 2006.

---

<sup>3</sup> NIST Special Publication 800-18, December 1998.

## RESULTS

OCIO has established a comprehensive framework for ensuring the security of federal information systems within the Smithsonian Institution. In accordance with NIST standards, OCIO has developed minimum-security controls for the Institution, which include:

- Maintaining an inventory of federal major information systems and applications and identifying the levels of security appropriate to protect such systems and applications;
- Establishing an Institution-wide information security program prescribing security practices and acceptable system configuration requirements;
- Performing system certifications and accreditations to ensure that security controls are in place and functioning as intended;
- Annually assessing the risk of unauthorized access and disruption of information systems that support the operations of the Institution;
- Documenting an action plan to track remediation of security vulnerabilities identified in annual self-assessments, vulnerability tests, and OIG reports;
- Periodically testing and evaluating the effectiveness of information security policies and practices;
- Reporting and responding to security incidents;
- Providing security awareness training to inform employees and contractors of their responsibilities in complying with Institution security policies; and
- Establishing plans for ensuring continuity of operations for systems that support key operations of the Institution.

While the framework established by OCIO addresses all of the critical components needed to protect the Institution's federal information system assets, our evaluation identified the following areas where implementation of the Institution's security program could be improved:

- **Inventory of Major Systems.** OCIO's inventory captures major federal information technology (IT) investments that the Institution is required to report to OMB through the Exhibit 300 process. According to the Chief Information Officer (CIO), these systems account for about 94 percent of all federal IT expenditures. While OCIO's approach generally satisfies FISMA reporting requirements, we noted the inventory does not identify all key interfaces between systems and networks, or links with third parties.

- **Certification and Accreditation Process.** Systems were certified and accredited without meeting all minimum security controls required by NIST and OMB guidance, and were not reaccredited when significant changes occurred in the information-processing environment. Also, none of the security plans for the 14 systems were updated to reflect the status of compliance with security configuration checklists, and only 4 of 12 security plans completed prior to FY 2005 were updated to reflect the self-assessment results or other changes. Of note, the security plan for the general support system was not updated nor a reaccreditation performed when new controls and services were implemented. Further, the Smithsonian Astrophysical Observatory (SAO)<sup>4</sup> system is hosted on Harvard University's network without an interconnection agreement that specifies the roles and responsibilities of the Institution and Harvard regarding the respective security controls that must be maintained.
- **Specialized IT Security Training.** According to the CIO, only 49 of the 81 individuals identified as having significant computer security responsibilities completed specialized security awareness training in FY 2005. OCIO relied on employee self-reporting at the end of the fiscal year and could not provide detailed information on courses taken and dates completed to document compliance with this requirement. To formally track specialized IT security training in FY 2006 the CIO will rely on the recently implemented training module in the Human Resources Management System.

Additionally, the following improvements are needed in OCIO's reporting practices to better facilitate our annual evaluation of the Institution's security program:

- **Action Plan.** OCIO's practice of removing completed action items in the subsequent reporting quarter makes it difficult for the OIG and OMB to evaluate the progress made in addressing system vulnerabilities. Keeping mitigated items on the action plan for a year would be more in line with reporting instructions issued by OMB.
- **Annual System Self-Assessments.** OCIO's and system owners' practice of completing annual self-assessments at the end of the fiscal year does not allow the Institution to adequately identify and mitigate security risks during the year through the action plan process. These assessments also occur too late for OIG consideration in its independent evaluation of the Institution's compliance with FISMA.

## SYSTEM INVENTORY DOES NOT IDENTIFY ALL OF THE INSTITUTION'S MISSION-CRITICAL SYSTEM INTERFACES

FISMA requires organizations to develop and maintain an inventory of major IT systems under their control or operated by a third party on their behalf, including all interfaces and links with other systems.<sup>5</sup> According to OMB, major systems include those that are important to the mission or function of an entity; are used for financial management and obligate more than \$500,000 annually; have significant program or policy implications; or have high executive visibility. The Smithsonian's IT security program is directed at those major systems in its inventory.

---

<sup>4</sup> SAO is a member of the Harvard-Smithsonian Center for Astrophysics and a research facility of the Smithsonian Institution.

<sup>5</sup> FISMA Section 305(c)(2)(c)(1) and (2).

In FY 2005, the CIO identified an inventory of 14 major systems comprising a general support system and 13 major applications, which he told us comprises about 94 percent of the Institution's federal IT expenditures. The inventory includes two applications added since the end of FY 2004—the Development and Membership Information System and the Human Resources Management System—and reflects only those systems that were reported to OMB on an Exhibit 300. According to the CIO, in November 2001, OMB agreed with the Institution's approach for identifying major systems.

While the inventory generally complies with FISMA reporting requirements, it does not identify all key interfaces between the major systems and links to external parties. For example, the inventory does not include Donate Now, an Internet application that sends individuals who donate funds to the Smithsonian to a third-party link for credit card authorization. Although this application does not handle a significant amount of funds, because it transmits sensitive data (personal identification and credit card information), it should be included in the Institution's inventory as a critical interface for purposes of security planning. The CIO indicated that Donate Now underwent a security review before it was deployed, as required. Nevertheless, Donate Now should have been identified as a critical interface in the Institution's major system inventory for FISMA reporting purposes.

### Recommendation

1. 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.

### CERTIFICATION AND ACCREDITATION PROCESS NEEDS IMPROVEMENT

NIST's *Guide for the Security Certification and Accreditation of Federal Information Systems*<sup>6</sup> outlines system certification and accreditation requirements. It states that organizations should conduct a risk assessment to evaluate the extent to which security controls in the information system are implemented correctly and operating as intended. Based on the results of the risk assessment, management should update the system security plans as appropriate. This plan provides the security requirements of information systems and describes the controls in place for meeting those requirements. The organization should also prepare an action plan to correct known vulnerabilities in security controls.

NIST guidance further states that management's risk assessment, security plan, and action plan comprise the accreditation package. During the accreditation phase, authorization to operate the system is either granted or denied based on a determination of whether remaining system vulnerabilities pose an acceptable level of risk to the organization's operations. Finally, NIST guidance requires continuous monitoring of security controls and reaccreditation of systems when there is a significant change to the system and/or its operational environment.

---

<sup>6</sup> NIST Special Publication 800-37, May 2004.

Our evaluation identified the following areas where the Institution needs to strengthen its certification and accreditation process:

- None of the security plans for the 14 major systems were updated to reflect the status of compliance with the Institution's security configuration standards or major changes to systems and/or their operational environment.
- Six of the 14 major systems reviewed did not have finalized disaster recovery plans and 1 system had no disaster recovery plan. The IT Security Specialist confirmed the status of these plans. Further, while the CIO conducted a tabletop test of the disaster recovery plan for the general support system, a full cutover and recovery test would provide greater assurance that the plan will work. Since the CIO will have to revise and retest the disaster recovery plan when the general support system is relocated to Herndon, Virginia, he should perform a full cutover test after the move.
- SAO's system is hosted on the Harvard University network without an interconnection agreement between the Smithsonian and the university.
- The Institution did not reaccredit its general support system when new controls and services were implemented.

### Security Plans for the 14 Major Systems Were Not Updated

None of the 14 major systems were updated to reflect the status of compliance with security configuration checklists. NIST's *Guide for the Security Certification and Accreditation of Federal Information Systems*<sup>7</sup> requires IT security plans to contain the most up-to-date information about the security of information systems. Although the frequency of system security plan updates is at the discretion of the system owner, major changes to an information system should be reflected in the system security plan. The CIO acknowledged that system security plans were not updated to reflect the status of configuration compliance. However, he indicated that as the accrediting official, he is aware of the status of configuration compliance of the major IT systems through alternate means. Nevertheless, NIST standards require that security plans be updated to provide system owners and senior officials assurance that effective security controls are in place. Doing so provides full accountability for any adverse impacts to organizations should a breach of security occur. The security plans also guide any future security certification and accreditation activities.

In addition, we noted that the security plan for the Institution's general support system had not been updated since September 10, 2003, even though OCIO expanded migration of servers to Active Directory, purchased and migrated SIRIS software to new servers, implemented new system controls and services, and installed firewalls. As a general practice, OCIO should be updating system security plans as necessary based on the results of the annual self-assessments, other changes, and include compliance with security configuration standards. As discussed later in this report, the Institution conducts self-assessments at the end of the fiscal year—too late in the FISMA reporting cycle to determine whether deficiencies noted should have been addressed in security plan updates.

---

<sup>7</sup> NIST Special Publication 800-37, May 2004.

In January 2006, after our review was completed, the CIO provided us three security plan updates that were not made available to us during our evaluation—one for the Institution’s Network Infrastructure, another for the Financial Enterprise Resource Planning System, and a third for the Facility Management System.

### **Systems are Operating without Finalized Disaster Recovery Plans**

A key element of a system security plan is a disaster recovery or contingency plan that describes the organization’s arrangement for ensuring system continuity in the event of a service disruption. Further, NIST’s *Contingency Planning Guide for Information Technology Systems*<sup>8</sup> provides that contingency plans should be tested to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan.

We determined that seven major applications were authorized to operate without completed and approved disaster recovery plans. At the time of our review, the plans for the National Museum of Natural History collection information system, the National Museum of American Indian collection information system and its registration information tracking system were stamped draft. Plans for the collection information systems of the National Museum of American History, National Air and Space Museum, and the Smithsonian Art Museums (ArtCIS) were undated. In January 2006, the CIO provided us with additional documentation to show that there were viable plans for six of the seven major applications and stated that the seventh plan for the National Postal Museum’s collection information system was included in the ArtCIS disaster recovery plan. However, none of these documents demonstrated that the disaster recovery plans had been finalized (i.e. plans were undated, stamped draft, and/or lacked approval signatures). In our view these plans should be presented as final documents and include appropriate approvals for accountability purposes.

We also found that the CIO performed a tabletop test of the general support system’s disaster recovery plan, instead of a full cutover and recovery test. While the tabletop testing method is generally acceptable, it requires only a walk-through of the procedures without the execution of actual recovery operations, and thus does not provide the same level of assurances that a functional cutover exercise would provide. Therefore, the Institution only has limited assurance that the major applications hosted thereon will maintain connectivity should a major disruption occur. Because the Institution’s major applications rely on the general support system to operate, the CIO may want to consider performing more substantive functional exercises, such as a system cutover as part of the pending relocation of the Institution’s data center and general support system to Herndon, Virginia.

### **SAO Operates on a Non-Smithsonian System without an Interconnection Agreement**

OCIO accredited the SAO Scientific Computing System to operate on a non-Institution network without an interconnection agreement with Harvard University specifying the roles and responsibilities of the Smithsonian Institution and Harvard regarding security controls that the university must maintain. OMB Circular A-130, Appendix III, requires organizations to obtain written management authorization before connecting their IT systems to other systems, based on

---

<sup>8</sup> NIST Special Publication 800-34, June 2002.

an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection and be included in the organization's system security plan.

If the university network is compromised, the interconnection could be used as a conduit to compromise the Institution's data as SAO has access to the general support system and the Financial and Human Resource Management Systems through an interconnection with Harvard's network. Without a documented interconnection agreement that details the rules of behavior<sup>9</sup> and the security controls that must be maintained by the interconnecting systems, the Institution does not know whether there is an acceptable level of risk. Further, the Institution has not complied with OMB requirements for completing an adequate system security plan.

### Significant System Changes Occurred with No Reaccreditation

We found that OCIO did not reaccredit the Institution's general support system after it underwent significant changes. NIST's *Guide for the Security Certification and Accreditation of Federal Information Systems*<sup>10</sup> stipulates that a system should be reaccredited periodically whenever there is a significant change to the system or its operational environment. Examples of significant changes that could trigger reaccreditation include the installation of a new or upgraded operating system, middleware component, or application; modifications to system ports, protocols, or services; and the installation of a new or upgraded hardware platform or firmware component. Changes in laws, directives, policies, or regulations, while not always directly related to the information system, can also potentially affect the security of the system and trigger a reaccreditation action.

In response to the OIG's security audit of the Institution's general support system,<sup>11</sup> OCIO implemented new system controls and services, and installed firewalls. Additionally, OCIO expanded the migration of servers to Active Directory and migrated SIRIS software to new servers. While individually these changes may not merit a reaccreditation, in our view, taken collectively a reaccreditation is warranted to determine if the security controls were negatively affected by these changes. This has far-reaching implications because all applications hosted on the general support system are vulnerable to any security weaknesses that may exist on the general support system due to these changes. Because the Institution's data center and general support system are being relocated to Herndon, Virginia in FY 2006, a reaccreditation of the system should not occur until after the move.

### Recommendations

We recommend that the CIO:

2. 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.

---

<sup>9</sup> The rules of behavior should clearly delineate the responsibilities and expected behavior of all individuals with access to the system and state the consequences of noncompliance.

<sup>10</sup> NIST Special Publication 800-37, May 2004.

<sup>11</sup> Report Number A-04-05, *Audit of the Smithsonian Institution Network Information System Controls*, Office of the Inspector General, January 6, 2005.

3. 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.
4. 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 *Security Guide for Interconnecting Information Technology Systems*.<sup>12</sup>
5. 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. 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.

### **SPECIALIZED IT SECURITY TRAINING NOT PROVIDED TO ALL EMPLOYEES WITH SIGNIFICANT COMPUTER SECURITY RESPONSIBILITIES**

NIST guidance<sup>13</sup> requires training for individuals whose roles in the organization indicate a need for special knowledge of IT security threats, vulnerabilities, and safeguards. In FY 2005, the Institution identified 81 individuals who had security-related duties with major information systems. According to the CIO, these individuals were given access to online computer security training and at the end of the fiscal year were required to self-identify training completed during the year. Of the 81 individuals, only 49 reported they had taken advanced security-related training. Tracking reports OCIO provided to us did not capture courses taken, hours of training completed, or course dates—information that would be needed to provide assurances that the training was sufficient to satisfy NIST requirements.

The CIO informed us that a training module was added to the Human Resource Management System in September 2005 to track all training, including computer security training information, for users with significant computer security responsibilities.

### **Recommendation**

We recommend that the CIO:

6. 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.
7. Ensure, either through OCIO's current tracking process or the Human Resource Management System, that in FY 2006 individuals identify course titles, hours, and completion dates of specialized IT training to provide assurances that NIST training requirements are satisfied.

---

<sup>12</sup> NIST Special Publication 800-47, August 2000.

<sup>13</sup> NIST Special Publication 800-16, *Information Technology Security Requirements: A Role-Based Performance Model*, April 1998, and NIST Special Publication 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003.

## IMPROVEMENTS NEEDED TO FACILITATE THE ANNUAL FISMA EVALUATION PROCESS

### Completed Action Plan Items Need to be Retained for a Minimum of One Year

OCIO maintains a consolidated list of system action items for the Institution, which it updates quarterly, as required by OMB. OCIO uses this list to track identified vulnerabilities related to major IT systems. OCIO removes “completed” action items in the reporting quarter subsequent to when the action was taken, and relies on program managers to maintain documentation of completed action plan items. Removing completed items quarterly makes OIG’s and OMB’s assessments of progress more difficult by requiring a comparison of quarterly reports to identify the total number of deficiencies remediated. OMB’s *FY 2004 Reporting Instructions for the Federal Information Security Management Act*<sup>14</sup> advises that deficiencies that have been completely mitigated for over a year should no longer be reported in the Institution’s action plan. While the guidance does not expressly require that items remain on the list for a year after deficiencies are corrected, doing so will provide a better audit trail for tracking the progress of the Institution’s remediation activities, expedite the OIG’s annual FISMA evaluation, and facilitate OMB’s oversight of the Institution’s IT security program.

### Self-Assessments

FISMA Section 3544(b)(5) requires each organization to assess annually the effectiveness of its information security policies, procedures, and practices. This assessment should include tests of its management, operational, and technical controls.

We found that the Institution performed these assessments as required by NIST. However, because all but one of these assessments were completed at the end of the fiscal year, they were not available for review during OIG’s FISMA evaluation or for inclusion in OCIO’s FISMA report to OMB, which is due by the beginning of October each year. Consequently, deficiencies discovered during the self-assessment process cannot be fully addressed in updates to the system security plans, risk assessments, and action plans until after the FISMA reporting deadlines. The CIO has agreed that the self-assessments need to be completed earlier and indicated that he will encourage system owners to complete self-assessments by July 30 of each year. This change will facilitate the OIG’s annual FISMA evaluation and provide for more timely updates of security plans when significant changes occur.

### Recommendations

We recommend the CIO:

8. Keep completed items in the action plan for one year after they have been fully mitigated.
9. Ensure self-assessments are completed and available no later than July 30 of each year.

---

<sup>14</sup> OMB Memorandum 04-25, August 23, 2004.

## MANAGEMENT COMMENTS

We provided management a draft report on January 20, 2006, and received formal written comments on February 7, 2006. Management's comments are included in their entirety in the Appendix to this report.

Management generally agreed with the report findings and conclusions related to its major system inventory, tracking of specialized IT security awareness training, and improvements needed in the timing of annual self-assessments. However, management disagreed with deficiencies we noted in its certification and accreditation process and the need to retain for 1 year mitigated IT security weaknesses on its Plan of Action and Milestones Report.

Specifically, management does not agree that major IT systems were accredited without disaster recovery plans or that the general support system (IT infrastructure) needed to be re-accredited because new controls and services were added. The CIO believes there were no significant changes to the hardware, software, or firmware during FY 2005 that warranted a recertification of the general support system. Also, while OCIO acknowledges it needs to clean up its paperwork, it contends that disaster recovery plans did exist for all of the seven major systems discussed in the report. Management stated that the OIG's concern that the plans were not dated or were stamped "draft" is form over substance, and that the Postal Museum collection information systems plan was combined with the ArtCIS plan. Furthermore, in reference to our recommendation on reporting mitigated security weaknesses, management does not agree with the IG's position that these should be retained for 1 year on the FISMA Plan of Action and Milestones Report.

Despite these disagreements, management concurred with recommendations 1, 2, 3, 4, 6, 7, and 9; partially concurred with recommendation 5; and non-concurred with recommendation 8. In its response, management stated that implementing the report's recommendations will strengthen the Institution's security accreditation process for major IT systems. Management's planned actions are summarized below:

**Recommendation 1.** The CIO agreed to include IT system interfaces in its major system inventory by February 10, 2006. However, the CIO disagrees that Donate Now is a major IT system for reporting purposes as it is not critical to the Institution's operations, costs far less than \$500,000 to operate annually, and has brought in less than \$40,000 in donations since October 2004.

**Recommendation 2.** OCIO states there is not a requirement to update system security plans unless there is a significant change. However, it will revise the Technical Standard and Guideline IT-930-01, IT Security Planning, by April 30, 2006, to require annual updates to security plans to document compliance with the Institution's security configuration standards.

**Recommendation 3.** OCIO stated that it would create a separate disaster recovery plan for the National Postal Museum's collection information system by February 10, 2006, but did not indicate whether it would finalize disaster recovery plans for six other major applications.

**Recommendation 4.** OCIO agreed to work with SAO and Harvard University to establish an interconnection agreement by July 30, 2006. In subsequent discussions, the CIO told us he also plans to establish an interconnection agreement with National Finance Center for payroll services.

**Recommendation 5.** OCIO will re-accredit the IT infrastructure and affected major IT systems once the relocation to Herndon, Virginia is complete.

**Recommendation 6.** OCIO stated it will work with OHR to ensure that Individual Development Plans for employees with specialized IT security training needs include IT security training and to monitor results.

**Recommendation 7.** OCIO will work with the Director of OHR to ensure IT security training reports identify course titles, hours, and completion dates.

**Recommendation 8.** OCIO does not believe there is a reporting requirement to retain completed items on the action plan for a year after they have been fully mitigated, and plans no action in response to the recommendation.

**Recommendation 9.** OCIO will revise the self-assessment guidance to require completion of the assessments by July 30 of each year.

## OFFICE OF THE INSPECTOR GENERAL RESPONSE

In evaluating management comments to this report, we held several discussions with the CIO and the IT Security Director in an effort to clarify the areas of disagreement. We continue to believe that the CIO should have reaccredited the general support system. In addition to installing firewalls and migrating servers to Active Directory, the CIO made several changes to network security and to operating and application configurations in response to our January 2005 audit of the Institution's network controls,<sup>15</sup> which should have triggered a reaccreditation. Nevertheless, the OIG and OCIO agree that the move of the data center and general support system to Herndon, Virginia, will require reaccreditations of many of the Institution's major IT systems.

We are encouraged that management recognizes the need to improve its documentation of system disaster recovery plans. While the CIO downplayed the importance of finalizing these plans, FISMA evaluation guidance requires that we review evidence of completion of these plans. The fact remains that the plans presented to us during our review and again in January 2006 were stamped draft, undated, and/or lacked approval signatures. After issuing our draft report, we learned that OCIO had finalized the remaining six disaster recovery plans. We will revisit this issue in our FY 2006 FISMA evaluation.

Management also did not agree to include Donate Now in its IT inventory for FISMA reporting purposes. We note that FISMA requires the identification of interfaces with each major system in the organization's inventory, including those not operated by or under the control of the organization. Although Donate Now is not a major system, it is an interface on numerous Institution sites that directs the public to a third party that begins a credit card authorization process. The sensitivity of the data captured combined with the link to a third party elevates the importance of this interface. Our FY 2006 FISMA evaluation will look closely at the Institution's inventory to ensure that it identifies all interfaces.

---

<sup>15</sup> Report Number A-04-05, *Audit of the Smithsonian Institution Network Information System Controls*, Office of the Inspector General, January 6, 2005.

Finally, management disagreed that fully mitigated items need to remain on the CIO's Plan of Action and Milestones Report for 1 year. Because this disagreement centers on an interpretation of OMB guidance, we plan to seek clarification from OMB on its reporting instructions.

Management's planned actions for recommendations 1 through 7, and 9, are responsive to the intent of our recommendations and we consider them resolved. However, we will continue to hold discussions with OCIO regarding the inclusion of Donate Now in its inventory for FISMA reporting. In addition, until we obtain clarification from OMB on its FISMA reporting instructions, recommendation 8 will remain unresolved.

We appreciate the courtesy and cooperation of Smithsonian representatives during this evaluation. If you have any questions concerning this report, please call me at (202) 275-2154 or Stuart Metzger at (202) 275-2159.

## APPENDIX. MANAGEMENT COMMENTS



Smithsonian Institution

Memo

Date February 7, 2006

To Debra Ritt, Inspector General

cc Sheila Burke, Deputy Secretary and Chief Operating Officer

From *Dennis R. Shaw*  
Dennis R. Shaw, Chief Information Officer

Subject Response to the Draft Report, Office of the Inspector General Audit M-05-03,  
Review of Smithsonian Institution Information Security Practices

Thank you for the opportunity to comment on the draft audit report on the Institution's information security practices. While we disagree with some of the audit findings and conclusions with respect to the need to re-certify major IT systems, we do agree that implementing the report's recommendations will strengthen the Institution's security accreditation process for major IT systems.

In the attachment, each issue presented in the audit report is addressed in order. Please me at 202-633-2800 or Bruce Daniels, Smithsonian Computer Security Manager, at 202-633-6000, if you have any questions.

Attachment

**APPENDIX. MANAGEMENT COMMENTS (CONTINUED)**

Attachment

**Issue 1: System inventory does not identify all of the Institution's mission-critical system interfaces**

"OCIO's inventory captures major federal information technology (IT) investments that the Institution is required to report to OMB through the Exhibit 300 process, according to the Chief Information Officer (CIO), these systems account for about 94 percent of all federal IT expenditures. While OCIO's approach generally satisfies FISMA reporting requirements, we noted the inventory does not identify all key interfaces between systems and networks, or links with third parties." \*\*\* In addition, the inventory does not include Donate Now, an Internet application that sends individuals to a third-party link for credit card authorization to donate funds to the Smithsonian.

**Response:** We agree that the IT system inventory should identify system interfaces. The IT system inventory is maintained in Chapter 5 of the Smithsonian Information Technology Plan and is updated annually. "Donate Now" is included in the Smithsonian Information Technology Plan and underwent a security review before it was implemented. However, we disagree that "Donate Now" is a major IT system for FISMA reporting purposes. It is not critical to the Institution's operations, costs far less than \$500,000 to operate annually, and has brought in less than \$40,000 in donations since October 2004.

**Issue 1 Recommendation**

**Recommendation 1:** We recommend the CIO identify and include all critical system interfaces in its major system inventory to comply with FISMA reporting requirements.

**Comment:** Concur. Section 5.5 of the FY 2006 – FY 2011 Smithsonian IT Plan will identify IT system interfaces.

**Target Completion Date:** February 10, 2006

**Issue 2: Certification and Accreditation Process Needs Improvement**

"Systems were certified and accredited without meeting all minimum security controls required by NIST and OMB guidance, and were not reaccredited when significant changes occurred in the information-processing environment. For example, 6 of the 14 major systems reviewed were granted full accreditation without finalized disaster recovery plans and 1 system had no disaster recovery plan. Also, none of the security plans for the 14 systems were updated to reflect the status of compliance with security configuration checklists as well as major system and/or operating environment changes. Of note, the security plan for the general support system was not updated nor a reaccreditation performed when

**APPENDIX. MANAGEMENT COMMENTS (CONTINUED)**

new controls and services were implemented. Further, the Smithsonian Astrophysical Observatory (SAO) system is hosted on Harvard University's network without an interconnection agreement that specifies the roles and responsibilities of the Institution and Harvard regarding the respective security controls that must be maintained. "

**Response:** We do not agree with the IG's findings that major IT systems were accredited without disaster recovery plans in place or that the general support system (IT infrastructure) needed to be re-accredited because new controls and new services added.

We believe that the certification and accreditation process is generally consistent with OMB and NIST guidance. OMB guidance requires re-certification every three years or when there is a significant change in the information system hardware, software, firmware, or surrounding environment. The IT Infrastructure (general support system) was certified in September 2004 after we implemented the perimeter firewall and Intrusion Detection System. There were no significant changes to the hardware, software, or firmware during FY 2005 that warranted a re-certification. The IG report cited the implementation of Microsoft Active Directory as a significant change. Active Directory was first deployed at SERC in July 2002 to support e-mail, and file and print services and at the SI units in the New York City area in August 2003 to support file and print services. While we have more units migrated to Microsoft Active Directory/Exchange/Outlook, the security controls do not change. We did install a firewall to separate NZP from the rest of SInet in 2005, however, that is not a significant change that warrants re-certification – it also enhances security.

The IG concluded that because several of the disaster recovery plans were not dated or stamped "draft" the systems should not have been accredited. The SI Computer Security Manager reviewed the disaster recovery plans with the system managers. We believe that this is clearly "form over substance", however, we agree that we need to clean up our paperwork. Also, the National Postal Museum Collections Information System (CIS) disaster recovery plan was combined with the ArtCIS disaster recovery plan because both share the same production environment and system administrator, and have the same controls. NPM staff are listed as part of the recovery team in the plan. We have revised the plan to indicate that it is a combined disaster recovery plan. OCIO has added the following dates to the Disaster Recovery Plans of NMAH CIS 10/2/2003, NASM CIS 6/10/2003, and ArtCIS 10/6/2003 and deleted "draft" from the Disaster Recovery Plans of NMAI CIS and NMNH RCIS,

**APPENDIX. MANAGEMENT COMMENTS (CONTINUED)****Issue 2 Recommendations**

We recommend that the CIO:

**Recommendation 2:** 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.

**Comment:** Concur. While there is no requirement to update the security plan on an annual basis unless there is a significant change, OCIO will revise the Technical Standard and Guideline IT-930-01, IT Security Planning, to require annual updates to document compliance with the Institution's security configuration standards and the results of annual self-assessments.

**Target Completion Date:** April 30, 2006

**Recommendation 3:** Develop a 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.

**Comment:** Concur. OCIO will create a separate disaster recovery plan for the National Postal Museum's Collections Information System.

**Target Completion Date:** February 10, 2006

**Recommendation 4:** Establish an interconnection agreement between the Smithsonian and Harvard University for the SAO Scientific Computing System as required by NIST's *Security Guide for Interconnecting Information Technology Systems*.

**Comment:** Concur. OCIO will work with SAO and Harvard University to establish an interconnection agreement.

**Target Completion Date:** July 30, 2006

**Recommendation 5:** Ensure that the general support system and affected major applications are reaccredited in FY 2006 after the primary data center and general support system are relocated to Herndon, Virginia. 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.

**APPENDIX. MANAGEMENT COMMENTS (CONTINUED)**

**Comment:** Partially Concur. OCIO will re-accredit the IT Infrastructure and affected major IT systems once the relocation to Herndon, VA is complete. Current IT security management processes require major IT systems be reaccredited when significant changes occur in systems and/or their operating environment.

**Target Completion Date:** July 30, 2006

**Issue 3: Specialized IT Security Training Not Provided to All Employees with Significant Computer Security Responsibilities**

"According to the CIO, only 49 of the 81 individuals identified as having significant computer security responsibilities completed specialized security awareness training in FY 2005. OCIO relied on employee self-reporting at the end of the FY and could not provide detailed information on courses taken and dates completed to document compliance with this requirement. The CIO hopes to have a formal tracking system in place for reporting such training for the FY 2006 FISMA review."

**Response:** OCIO's tracking of specialized IT security training was designed to meet FISMA reporting requirements. FISMA reporting requires each agency to identify the number of employees with IT security responsibilities, how many took IT security training, and how much it costs. The IG's recommendation to expand the data we collect is reasonable, but not required for the annual FISMA report. OCIO also notes that the training is not an annual requirement – if the employee completed specialized training in 2005, the same training does not have to be taken in 2006. The HRMS Training module should help with obtaining the additional information assuming that SI units actually report it. On a more general note, each employee should have an Individual Development Plan (IDP) and for those employees with a need for specialized IT security training, the IDP should include it. We believe that the IT security training available through USA Learning is sufficient to meet IT security training needs.

**Issue 3 Recommendations**

We recommend that the CIO:

**Recommendation 6:** 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.

**Comment:** Concur. OCIO will work with OHR to ensure that the Individual Development Plans of employees with specialized IT security training needs include IT security training. OCIO will also work with OHR to monitor results.

**APPENDIX. MANAGEMENT COMMENTS (CONTINUED)**

**Target Completion Date:** December 31, 2006

**Recommendation 7:** Ensure, either through OCIO's current tracking process or the Human Resource Management System, that in FY 2006 individuals identify course titles, hours, and completion dates of specialized IT training to provide assurances that NIST training requirements are satisfied.

**Comment:** Concur. OCIO will work with the Director, OHR that reporting of IT security training identifies course titles, hours, and completion dates.

**Target Completion Date:** July 30, 2006

**Issue 4: Improvements Needed To Better Facilitate the Annual FISMA Reporting Process**

"OCIO's practice of removing completed action items in the subsequent reporting quarter makes it difficult for the OIG and OMB to evaluate the progress made in addressing system vulnerabilities. Keeping mitigated items on the action plan for a year would be more in line with reporting instructions issued by OMB. OCIO's practice of completing annual self-assessments at the end of the fiscal year does not allow it to adequately identify and mitigate security risks during the year through the action plan process. These assessments also occur too late for OIG consideration in its independent evaluation of the Institution's compliance with FISMA."

**Response:** Mitigating security weaknesses in a continuous process. We believe that the issue is not whether OCIO has sufficient time, but whether the auditors can review what was done in time to meet FISMA reporting deadlines imposed by OMB. OCIO relies on the system owner to conduct the self-assessments. OCIO will revise the self-assessment guidance to require completion by July 30<sup>th</sup> of each year and encourage system owners to get them done sooner in the fiscal year.

We do not agree with the IG's position that mitigated weaknesses must be retained on the FISMA Plan of Action and Milestone Report (POAM) for a year.

**Issue 4 Recommendations**

We recommend that the CIO:

**Recommendation 8:** Keep completed items in the action plan for one year after they have been fully mitigated.

**APPENDIX. MANAGEMENT COMMENTS (CONTINUED)**

**Comment:** Non-Concur. There is no FISMA reporting requirement to do this. All quarterly reports are available and the auditors can review all 4 quarterly reports.

**Target Completion Date:** Not Applicable

**Recommendation 9:** Ensure self-assessments are completed and available no later than July 30<sup>th</sup> of each year.

**Comment:** Concur. OCIO will revise the self-assessment guidance to require completion by July 30<sup>th</sup> of each year and encourage system owners to get them done sooner in the fiscal year.

**Target Completion Date:** July 30, 2006