



Office of the Inspector General

Date May 16, 2007

To Cristián Samper, Acting Secretary

Cc Sheila P. Burke, Deputy Secretary and Chief Operating Officer
Virginia Clark, Director, Office of External Affairs
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 Development and Membership Information System Audit, Number A-06-08

Attached please find a copy of our final report on the FY 2006 FISMA audit of the Development and Membership Information System (DMIS). We made two recommendations to strengthen the confidentiality, availability, and integrity of the information on DMIS and to enhance audit trails and user accountability. Management fully concurred with the report findings and recommendations and has planned or taken action that will resolve the recommendations.

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

AUDIT REPORT
**Development
And
Membership Information System**

Number A-06-08

May 16, 2007



Smithsonian Institution

Office of Inspector General



In Brief

Development and Membership Information System

Report Number A-06-08, May 16, 2007

Why We Did This Evaluation

The Federal Information Security Management Act of 2002 (FISMA) directs the Office of the Inspector General to annually evaluate the information security program of the Institution. The Institution voluntarily complies with FISMA requirements because it is consistent with its strategic goals. FISMA outlines federal information security compliance criteria, including the requirement for a review of a subset of systems as part of the annual independent assessment by the Institution's Inspector General. This report covers the evaluation of the DMIS technical security controls and supports the Smithsonian Institution Office of the Inspector General (OIG) annual FISMA evaluation of the information security controls implemented by the Institution.

What We Recommended

We made recommendations to strengthen the confidentiality, availability, and integrity of the information on DMIS and to enhance audit trails and user accountability.

Management fully concurred with the report findings and recommendations. Management has planned or taken action that will mitigate the identified weaknesses.

What We Found

The Development and Membership Information System (DMIS) is a commercial off-the-shelf information system application that is used by the Office of Development and staff across the Institution to support constituency research, gift recording, membership, and other related development services. The data in DMIS is confidential because it contains information relating to Smithsonian Institution donors, prospects, and members.

We identified several areas in which adequate controls have not been documented and put in place. For instance, standard security configuration baselines have not been implemented and account administration controls are weak. As a result of failing to implement standard configuration baselines, many areas of weakness exist that would likely have been addressed or mitigated had one been implemented.

Regarding account administration controls, we found that Administrators are logging into the system through a shared Administrator account rather than having each user assigned an individual ID so that server actions can be tracked and user accountability can be established. The use of shared or group accounts minimizes or eliminates the effectiveness of audit trails, because actions cannot be tied back to a single individual. Individuals who use group accounts or share a single ID could potentially perform unauthorized or inappropriate activities within the system that could not be tied back to them.

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

For additional information or a copy of the full report, contact the Office of the Inspector General at (202) 633-7050 or visit <http://www.si.edu/oig>.

**REPORT ON REVIEW OF
FISCAL YEAR 2006
DEVELOPMENT AND MEMBERSHIP INFORMATION SYSTEM
SMITHSONIAN INSTITUTION
OFFICE OF THE INSPECTOR GENERAL**

Cotton & Company LLP
Auditors · Advisors
635 Slaters Lane, 4th Floor
Alexandria, Virginia 22314
www.cottoncpa.com

CONTENTS

Section	Page
Purpose	1
Background	1
Objectives, Scope and Methodology	2
Summary of Results:	
1. Standard Security Configuration Baselines have not Been Implemented	4
2. DMIS Account Administration Controls are Weak	5
Summary of Management Response	6
Office of the Inspector General Comments	6
Appendix – Management Response	7

**REPORT ON REVIEW OF
FISCAL YEAR 2006
DEVELOPMENT AND MEMBERSHIP INFORMATION SYSTEM
SMITHSONIAN INSTITUTION
OFFICE OF THE INSPECTOR GENERAL**

Cotton & Company LLP conducted an audit of the Smithsonian Institution's Development and Membership Information System (DMIS) technical security controls in support of the Office of the Inspector General's overall responsibilities related to Title III of the 2002 E-Government Act, also known as the Federal Information Security Management Act.

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 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 covers the evaluation of the DMIS technical security controls and supports the Smithsonian Institution Office of the Inspector General (OIG) annual FISMA 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* 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 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.

- **System Security Plan.** NIST's *Guide for Developing Security Plans for Information Technology 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 DMIS. We conducted this audit in accordance with *Generally Accepted Government Auditing Standards*, 2006 Revision, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This report is intended to meet the objectives described below and should not be used for other purposes.

DMIS, a commercial off-the-shelf application based on the Sage Software product "Millennium," is used by the Office of Development and staff across the Institution to support, manage, and control constituency research, gift recording, membership, and other related development services. DMIS information is confidential, because it contains names and addresses of donors, prospects and members, and in some cases credit card information. It also contains confidential information about interactions with donors, prospects, and members and other giving information.

The objectives of this independent audit were to evaluate and report on the existence and effectiveness of technical security controls over DMIS and to determine if baselines had been adequately documented and implemented over the DMIS operating system and database. To accomplish these objectives, we performed detailed reviews of the DMIS Oracle (Oracle 9i) database and Windows 2003 server supporting the database. In addition, we performed a high-level review of available certification and accreditation (C&A) documentation, including the DMIS:

- System Security Plan
- Plan of Action and Milestones (POA&M)
- Risk Assessment
- Certification and Accreditation Letters
- Documented NIST SP 800-53 Mandatory Controls

For the Oracle database, we conducted interviews with the DMIS project manager and database administrator and performed a security configuration review of the DMIS Oracle 9i database that serves as the back-end for the application. We conducted the database review in two phases.

- In the first phase, we reviewed OCIO's Oracle security baseline, Security Settings for Oracle Servers. This document outlines recommended security settings for Oracle database installations at the Institution.

- In the second phase, we compared the current security configuration of the DMIS Oracle 9i database to baselines from the Institution and the Center for Internet Security's (CIS) Oracle benchmark. We also reviewed the DMIS baseline configuration using an automated database scanning tool (AppDetective).

DMIS consists of four Windows servers: web server, database server, reporting server, and document server. Our review focused on the database server's operating system running Windows 2003. Audit procedures consisted of interviewing the DMIS project manager and server administrator and completing a detailed configuration review of the server's operating system.

Finally, we reviewed DMIS C&A documentation as part of the overall FISMA evaluation to determine if it complied with Institution, NIST, and OMB criteria in content and form. At a high level we compared the DMIS system security plan to NIST Special Publication (SP) 800-18, *Developing Security Plans for Information Technology Systems* and OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources* to verify key requirements were being addressed.

In addition, we compared the DMIS POA&M to the Institution's Technical Standard and Guidelines, IT-930-01; NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Process*; OMB Circular A-130, Appendix III; and OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*.

RESULTS

DMIS received re-authorization to operate in August 2006 after completion of a formal recertification and reaccreditation process. As a result of the re-authorization, management updated the DMIS system security plan, POA&M, and other supporting documentation which were reviewed during the overall FISMA evaluation (see OIG's *FY 2006 FISMA Audit of the Smithsonian Institution's Information Security Program*, Audit Report Number A-06-05). Although our overall review of the Institution's C&A documentation did not identify any significant issues with the C&A process or more specifically the DMIS C&A documentation, we did identify two issues in the overall FISMA evaluation report which were in part supported by DMIS weaknesses and made recommendations on those issues.

Specifically, as noted in the FY2006 FISMA evaluation report, the DMIS system security plan did not include or make reference to common security controls; however, these controls were identified in a separate document. Additionally, the report noted that controls were not adequate to ensure standard security configuration baselines had been implemented on the Institution's major applications in accordance with Institution policy. In fact, DMIS was an example of a system on which baselines were not implemented.

This report documents the results of technical testing conducted on the DMIS Windows operating system and Oracle database which support the DMIS web server as well as our associated recommendations. We noted several areas in which adequate controls have not been documented and put in place. For instance, standard security configuration baselines have not been implemented, and account administration controls are weak.

Standard Security Configuration Baselines Have Not Been Implemented

NIST SP 800-70, *Security Configuration Checklists Program for IT Products*, states:

A security configuration checklist (sometimes called a lockdown or hardening guide or benchmark) is in its simplest form a series of instructions for configuring a product to a particular security level (or baseline)...The use of well-written, standardized checklists can markedly reduce the vulnerability exposure of IT products. Checklists may be particularly helpful to small organizations and individuals that have limited resources for securing their systems.

The Institution's OCIO had developed, documented, and posted on the Institution's intranet baselines for use by system owners when configuring their systems. In addition, OCIO developed and documented IT-960-TN16, which 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.

The Institution's standard security configuration baselines have not been implemented. Individuals responsible for administration of DMIS were aware of the standard security configuration baselines distributed by OCIO and had included them in the DMIS POA&M as a weakness. Our review of the DMIS POA&M noted that management identified timelines for implementing the baselines, as follows:

Reporting Server:	September 30, 2006
Document Server:	December 31, 2006
Database Server:	March 31, 2007
Web Server:	June 30, 2007

Further, these baselines have not been implemented as of the date of this report. As a result of failing to implement standard configuration baselines, many areas of weakness exist that would likely have been addressed or mitigated with the implementation of a standard security configuration baseline:

- The latest patchset had not been applied.
- Strong database password controls have not been implemented.
- Database-level auditing controls have not been enabled.

In addition, our review of the Windows 2003 server supporting the Oracle database identified weaknesses in the following areas, which again would likely have been addressed or mitigated if a standard security configuration baseline were in place over that server:

- Strong OS password controls have not been implemented.
- OS-level logging and auditing controls have not been implemented.
- Security policies are weak.
- File and registry permissions are not configured appropriately.
- Unnecessary services are identified as running on the server.

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

1. We recommend the DMIS System sponsor/owner promptly implement standard security configuration baselines for the DMIS Oracle database and for each server supporting DMIS, as soon as practicable. In addition, the DMIS system sponsor/owner should document on the baseline where recommended security controls have not been implemented and provide valid business reasons, and include the completed baseline in the system security plan as part of the C&A package.

DMIS Account Administration Controls Are Weak

Controls are not adequate to ensure that individuals logging into the DMIS Windows 2003 server are logging in through individual accounts specifically assigned to them. Administrators are logging into the system through a shared Administrator account rather than having each user assigned an individual ID so that server actions can be tracked and user accountability can be established.

Smithsonian Directive (SD) 931, *Use of Computers and Networks – Required Safeguards*, states:

To protect Smithsonian equipment and data, users are required to use safeguards that include - Prohibiting system administrators from establishing group accounts controlled by a single password.

In addition, Technical Standard and Guideline IT-930-02, *Security Controls Manual*, Section 3.1.1.2, User IDs, states:

User IDs must be unique to an individual; no group user ID's are permitted. This control is essential for ensuring user accountability. System administrators will ensure that contractor and other non-staff personnel (e.g. interns and volunteers) have individual accounts and that these accounts are either set to expire at the end of the contract or internship, or that they are reviewed annually on the anniversary date of the establishment of the account to ensure that there is still a legitimate need for the account. Technical Note IT-960-TN10 specifies the procedures for User Creation Guidelines.

Further, Section 3.1.1.4, *Generic or Group IDs*, states:

User accounts and ID's must be unique to an individual. No group or shared accounts are permitted.

The use of shared or group accounts minimizes or eliminates the effectiveness of audit trails, because actions cannot be tied back to a single individual. Individuals who use group accounts or share a single ID could potentially perform unauthorized or inappropriate activities within the system that could not be tied back to them.

Recommendation

2. We recommend the DMIS system sponsor/owner require administrators to log into DMIS in accordance with Institution policy using individual accounts to enhance audit trails and user accountability.

Summary of Management Response

Management's April 19, 2007, response to our draft report concurred with both recommendations to strengthen the confidentiality, availability, and integrity of the information on DMIS and to enhance audit trails and user accountability. The Director, Office of External Affairs agreed to fully implement standard security configuration baselines within six months of receiving the latest operational release of Blade Logic (a software delivery and configuration utility used for Windows servers) from OCIO. Management also stated that it had established individual administrator accounts and that they were being used to enhance audit trails and user accountability. The full text of management's response is included in the Appendix.

Office of the Inspector General Comments

Management has planned and taken actions that respond to our recommendations, and we consider them resolved. In evaluating management's response to this report, we conferred with the IT Security Director and determined that the new version of Blade Logic was due to be released in July 2007. Therefore, we have established a target completion date for Recommendation 1 as January 31, 2008, 6 months from the date of the release. Additionally, OCIO should ensure that the POA&M is updated with the revised completion data as well.

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 – Management Response



Smithsonian Institution

Memo

Office of External Affairs

Date April 19, 2007

To A. Sprightley Ryan, Inspector General

cc Ann Speyer, Chief Information Officer
Bruce Daniels, Director of IT Security and Smithsonian Computer Security Manager

From Virginia Clark, Director, Office of External Affairs 

Subject Draft Report on the Fiscal Year 2006 Development and Membership Information System Audit, Number A-06-08

Thank you for the draft audit report on the FY 2006 FISMA audit of the Development and Membership Information System (DMIS), Number A-06-08.

Recommendation 1, Standard Security Configuration Baselines have not Been Implemented

Comment: Concur. Full implementation depends on the acquisition of the latest release of Blade Logic by OCIO. In the meantime, I have directed the Technology Team to work with OCIO's IT Security group to implement the current OS and database baselines on the DMIS production servers, and to document any necessary deviations from the baseline.

Target Completion Date: six months following operational implementation of Blade Logic's capability to show sever status against baseline.

Recommendation 2, DMIS Account Administration Controls are Weak,

Comment: Concur. Individual administrator accounts have been established and are being used on the DMIS production servers to enhance audit trails and user accountability.

Target Completion Date: Completed

Please let me know if you have any questions the response to this report.

Smithsonian Institution
SIB 121, MRC 027
PO Box 37012
Washington, DC 20013-7012
202.633.5021 Telephone
202.633.0183 Fax