

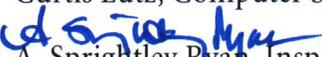


Office of the Inspector General

Date September 19, 2007

To Cristián Samper K., Acting Secretary

Cc Sheila P. Burke, Deputy Secretary and Chief Operating Officer  
Ann Speyer, Chief Information Officer  
James D. Douglas, Director, Office of Human Resources  
Deron S. Burba, Director, Systems Modernization  
Bruce A. Daniels, Director of IT Security and Smithsonian Computer Security Manager  
Curtis Lutz, Computer Scientist, Human Resources and Administrative Systems Division

From  A. Sprightley Ryan, Inspector General

Subject Report on the Fiscal Year 2007 Human Resources Management System (HRMS)  
Audit, Number A-07-06

Attached please find a copy of our final report on the FY 2007 FISMA audit of HRMS. We made five recommendations to strengthen controls over HRMS by enforcing Institution policies, procedures, and practices over the confidentiality, availability, and integrity of the system. Management concurred with the report findings and recommendations and has planned or taken action that will resolve the recommendations.

Please call Stuart Metzger or Joan Mockeridge at 202-633-7050 if you have any questions.

**AUDIT REPORT**

**Human Resources  
Management System**

Number A-07-06

September 19, 2007



**Smithsonian Institution**

**Office of Inspector General**



## In Brief

## Human Resources Management System Report Number A-07-06, September 19, 2007

### Why We Did This Evaluation

Under the Federal Information Security Management Act of 2002 (FISMA), the Office of the Inspector General (OIG) conducts an annual independent assessment of the Institution's information security system. As part of that assessment, FISMA requires a review of a subset of information systems. This report covers one such system, the Human Resources Management System (HRMS), and evaluates HRMS management, operational, and technical security controls.

### What We Recommended

We made five recommendations to strengthen controls over HRMS by enforcing Institution policies, procedures, and practices over user access request forms, segregation of employee duties, database logging and monitoring, system baselines, and interconnection agreements.

Management concurred with the report's findings and recommendations and has planned or taken action that will resolve all recommendations.

### What We Found

HRMS contains sensitive personnel data. Managers throughout the Institution use HRMS to manage core activities such as recruitment, electronic transmittal of personnel actions, benefits administration, training, and recording and reporting of workplace incidents and injuries.

Overall, we concluded that management has done a good job identifying, documenting, and implementing management, operational, and technical controls over HRMS. We did, however, note instances during our testing where policies and procedures were not being followed. Specifically, we found that:

- Management did not enforce access authorization procedures that require approved user access request forms, increasing the risk of individuals being granted excessive or unauthorized access to the system and related data.
- Management did not ensure adequate segregation of administrative and security functions, particularly duties concerning the review of database logs and access restrictions associated with system changes.
- Management did not review database logs or monthly compliance reports on a consistent basis, increasing the risk that inappropriate or unauthorized activities may have occurred without detection.
- Management did not document the final HRMS baselines and note where deviations may have occurred for valid business purposes. As a result, management cannot ensure that technical controls have been adequately identified and implemented.
- The Institution did not establish proper authorization for the HRMS connection with the National Finance Center, which was outside of the accreditation boundary.

Without adequate controls in place to enforce Institution policies, procedures, and practices over HRMS, the confidentiality, availability, and integrity of the system and its 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 THE AUDIT OF THE  
FISCAL YEAR 2007  
HUMAN RESOURCES MANAGEMENT SYSTEM  
SMITHSONIAN INSTITUTION  
OFFICE OF THE INSPECTOR GENERAL**

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	3
Background	3
Objectives, Scope, and Methodology	4
Results	
User Access Request Procedures Are Not Implemented	5
Segregation of Duty Controls Need Improvement	6
Database Logging and Monitoring Controls Are Inadequate	8
Baseline Configurations Are Not Documented	9
Information System Connections Are Not Formally Authorized	10
Summary of Management Response	12
Office of the Inspector General Comments	12
Appendix – Management Response	13

**REPORT ON THE AUDIT OF THE  
FISCAL YEAR 2007  
HUMAN RESOURCES MANAGEMENT SYSTEM  
SMITHSONIAN INSTITUTION  
OFFICE OF THE INSPECTOR GENERAL**

Cotton & Company LLP conducted an audit of the Smithsonian Institution's security management programs and practices to determine the effectiveness of management, operational, and technical security controls over the Institution's Human Resources Management System (HRMS).

**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 HRMS management, operational and 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:

- **Recommended Security Controls.** NIST's *Recommended Security Controls for Federal Information Systems* provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store, or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government. The process of selecting and specifying security controls for an information system includes the organization's overall approach to managing risk, the security categorization of the system in accordance with Federal Information Processing Standard (FIPS) 199 and the selection of minimum (baseline) security controls, the activities associated with tailoring the baseline security controls through the application of scoping guidance and the assignment of organization-defined parameters, and the potential for supplementing the minimum security controls with additional controls, as necessary, to achieve adequate security.
- **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 the 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, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.” NIST guidance also discusses system 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 agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an 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 HRMS, the Institution’s human resources system. We conducted this audit in accordance with *Government Auditing Standards, 2007 Revision*, as amended, 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.

As part of the Institution’s Enterprise Resource Planning (ERP) system, HRMS contains sensitive information that must be protected from unauthorized disclosure. The mission of HRMS is to help managers at all levels manage human resource information successfully. Managers throughout the Institution use the system to manage core activities including:

- Recruitment
- Electronic transmittal of personnel actions
- Benefits administration
- Training
- Employee and labor relations
- Recording and reporting of workplace incidents and injuries
- Management of relevant Occupational Health and Safety data
- Competencies, career planning, and succession planning

The objectives of this independent audit were to evaluate and report on management’s identification, documentation, and implementation of management, operational and technical security controls required by NIST Special Publication (SP) 800-53.

To accomplish these objectives, we performed a detailed audit of required controls using suggested audit procedures outlined in NIST's Draft SP 800-53A. We performed a high-level review of available certification and accreditation (C&A) documentation, including the HRMS:

- System Security Plan
- Plan of Actions and Milestones
- Risk Assessment
- Certification and Accreditation Letters, and
- Documented NIST SP 800-53 controls

Management has classified HRMS as a moderate-impact system in accordance with FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems*. The system and its data are sensitive. As a result, we evaluated HRMS general controls from November 2006 through January 2007 using test procedures for a moderate impact system as defined in NIST's Draft SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems*. Test procedures in SP 800-53A were designed by NIST to test specific security controls outlined in NIST SP 800-53 *Recommended Security Controls for Federal Information Systems*. We tested the controls defined by NIST SP 800-53 for such systems through interviews, observation, and specific testing procedures where applicable. Examples of key controls tested included:

- Controls over administration of user accounts
- Controls over application, database, and server changes
- Controls over segregation of duties within HRMS, and
- Controls over the logging and monitoring of user activities

## **RESULTS**

Overall, we concluded that management has done a good job identifying, documenting, and implementing management, operational, and technical controls over HRMS. Specifically, we noted that the HRMS C&A process was adequately documented, the Plan of Actions & Milestones (POA&M) was effectively maintained, and the HRMS disaster recovery plan had been adequately tested. We did, however, note some weaknesses during our testing. While policies and procedures have been established, in some instances these policies and procedures were not being followed, which may increase risks beyond what management is willing to accept. We detail these specific control weaknesses below.

### **User Access Request Procedures Are Not Implemented**

Controls are not adequate to ensure that policies and procedures over the use of user access request forms are implemented. We determined management was not enforcing their documented access authorization procedures that require new user access be requested and approved using the HRMS access request form. We selected a sample of 45 HRMS users and requested supporting access request forms and noted that of the 45 users selected, 44 users did not have an access request form. Upon further review, we noted that the 44 users had supporting emails, but these emails did not include all of the information contained in the access request form, such as a signature.

HRMS System Security Plan Section AC-2 *Account Management* states that:

To access the ERP HRMS system, a user must have an active Novell network logon ID/password and a PeopleSoft / Medgate logon ID/password. Users must submit a written and approved ERP HRMS access request form to the Help Desk to gain access to the system. Access request forms must be signed by the user's immediate supervisor and Administrative Officer. The supervisor and Administrative Officer are responsible for ensuring that the user's privileges are appropriate and that proper segregation of duties is maintained. The user's immediate supervisor is responsible for ensuring that user access privileges are removed in a timely manner.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems (AC Policies and Procedures)*, states that:

AC-2 Account Management: The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, section 3.5.2 (User Administration) under *User Account Management* states that:

Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Insufficient or ineffective access controls can increase the risk of individuals being granted excessive or unauthorized access to the system and related data, which increases the risk of inappropriate disclosure of sensitive data.

## **Recommendation**

1. We recommend that the Chief Information Officer (CIO) enforce the Institution and HRMS-specific access control policy which requires an approved ERP HRMS access request form be submitted prior to granting new users access to HRMS. In addition, all current users who do not have an approved access request form on file should be required to complete the form.

## **Segregation of Duty Controls Need Improvement**

Controls are not adequate to ensure that access within HRMS has been adequately segregated to reduce the likelihood of individuals performing inappropriate or unauthorized activities. Specifically, we determined management has not taken adequate steps to ensure the segregation of incompatible functions in HRMS. We noted the following weaknesses:

- Review of HRMS Oracle database logs is not performed by an individual independent of administration. Currently, database logs are reviewed by the Oracle database administrator. Best practices dictate that administrative and security functions be segregated to ensure activities performed by individuals with high-level access are independently reviewed.

- HRMS developers have access to the production environment. Specifically, we identified four individuals with access to the development, testing, and production environments in HRMS. We determined that OCIO can grant waivers for these individuals if it is necessary to have access to production to perform their job duties. Through interviews, we determined that these individuals did not have a waiver from OCIO justifying their level of access. NIST and industry best practices require sensitive activities, including the development of changes and movement of changes into production, be segregated to help ensure only authorized changes are introduced into production.

The HRMS system security plan section AC-5 *Separation of Duties* states that:

Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.

Where feasible, programmers who maintain an application should not have access to production data in that system. Programmers must not, in any case, alter data using processes external to the application without documented approval by the system sponsor. In sensitive systems users must not be given privileges that allow them to initiate and approve the same transaction.

In addition, Technical Note IT-930-TN10 details the procedures on minimizing access to production software and data, including separation of duties. Section C.ii *Separation of Duties* states:

Ensure that application developers and system administrators are not given access to modify production data. If this is required for their official duties, then a waiver must be obtained by OCIO.

Finally, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems (Policies and Procedures)* states:

CM-5 Access Restrictions for Change: The organization enforces access restrictions associated with changes to the information system.

Our review of the standard HRMS access request form noted that administrative activities and system support functions were not identified on the access request form. However, during the exit conference OCIO provided a revised access request form, which now identifies specific functions. Although these functions have been identified, not enforcing the concepts of least privilege or separation of duties with regards to the review of database logs and access restrictions associated with HRMS changes increases the risk of inappropriate activities occurring without management's knowledge.

## Recommendation

2. We recommend that the CIO identify, document, and implement segregation of duty controls for sensitive administrative and system support functions. Management should document in the system security plan those activities that need to be segregated.

### Database Logging and Monitoring Controls Are Inadequate

Controls are not adequate to ensure HRMS database logs are reviewed weekly as required by NIST and Institution auditing and logging policies and procedures. Specifically, we determined HRMS database logs were not being reviewed on a consistent basis.

We noted that monthly compliance reports are generated to report auditing and logging activities within HRMS but are not regularly reviewed. The monthly compliance reports show selected application and database auditing and logging activities that are monitored each month and submitted to OCIO. Based on our review of the November 2006 report, we noted that database log activities within HRMS were not included.

Technical Note IT-930-TN03, *Auditing & Logging Procedures* state:

Review logs weekly. Audit trails must be reviewed weekly by the Security Group or other authorized individuals who do not administer access to the application and/or system and are not regular users of the system. The Computer Security Manager must review the audit trail monthly and provide a report to OCIO. Anomalies must be reported immediately to appropriate supervisory positions and the Computer Security Manager for follow-up action. After resolution of any abnormalities a formal report of findings must be reported to OCIO.

In addition, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems (Access Controls)* states:

AC-13 Supervision & Review – Access Control: The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls. The organization reviews audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures. The organization investigates any unusual information system-related activities and periodically reviews changes to access authorizations. The organization reviews more frequently the activities of users with significant information system roles and responsibilities.

AU-6 Audit Monitoring, Analysis & Reporting: The organization regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions. The organization employs automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities.

Insufficient or ineffective monitoring of system logs can increase the risk that inappropriate or unauthorized activities may occur without management knowledge.

## Recommendation

3. We recommend that the CIO enforce Institution policy and procedures requiring the weekly review of logs and monthly submission of appropriately detailed management reports to OCIO.

## Baseline Configurations Are Not Documented

Controls are not adequate to ensure that differences between the Institution and HRMS baselines are documented. Specifically, we noted that while management used OCIO's standard baseline templates to install and configure HRMS, management did not document the final baselines and note where deviations may have occurred for valid business purposes.

In addition, as noted in the FY2006 FISMA evaluation report,<sup>1</sup> OCIO's standard baselines for Windows and Oracle were not adequate to ensure all controls applicable to Windows and Oracle systems were addressed.

NIST SP 800-40, *Creating a Patch and Vulnerability Management Program* Section 4.3 *Using Standardized Configurations* states that:

A standard configuration should be defined for each major group of IT resources (e.g., routers, user workstations, file servers). Organizations should focus standardization efforts on types of IT resources that make up a significant portion of their entire IT resources. Likely candidates for standardization include end user workstations, file servers, and network infrastructure components (e.g., routers, switches). The standard configuration will likely include the following items:

- Hardware type and/or model
- Operating system version and patch level
- Major installed applications (version and patch level)
- Standard configuration settings

In many cases, these standardized configurations can be maintained centrally, and changes can be propagated to all participating IT resources. An organization that relies on a hardware supplier to place a standard configuration on new computers should coordinate closely with that supplier to ensure that changes, including new patches, are implemented quickly.

In addition, OCIO Technical Note IT-960-TN16 *Baseline and Configuration Management of Application, Database, and Web Servers*, dated June 16, 2005 Section D *Server Configurations*, pg. 5 states:

---

<sup>1</sup> *Report on FY 2006 FISMA Audit of the Smithsonian Institution's Information Security Program*, Number A-06-05, April 20, 2007.

Individual server configuration documents must be maintained for each server by system owners. At a minimum, these documents should contain information such as the server name, location, purpose, Internet Protocol (IP) configurations, application specifics, organizations supported, maintenance schedules, and which baseline document was used to initially build the server.

Without system-specific documented baselines, management cannot ensure that technical controls have been adequately identified and implemented.

### **Recommendation**

4. We recommend that the CIO document final baselines for the HRMS operating system and database after determining what Institution-wide baselines will be adopted. In addition, as part of installing the baselines, OCIO should specifically note where suggested security settings have not been implemented for valid business purposes.

### **Information System Connections Are Not Formally Authorized**

Controls are not adequate to ensure that the Smithsonian establishes proper authorization for all connections from the information system to other information systems outside of the accreditation boundary and monitors and controls the system interconnections on an ongoing basis.

HRMS has been operating since October 2004 without any formal interconnection agreement with the National Finance Center (NFC). Sensitive privacy data related to personnel and workers' compensation issues is being transferred through the Institution's connections with NFC. Our audit determined that the Institution has an informal Interconnection Security Agreement (ISA) but no Memorandum of Understanding (MOU) with NFC. This issue has been included in the POA&M.

The Institution's policy on information system connections requires both an Interconnection Security Agreement and a Memorandum of Understanding. OCIO Technical Note IT-930-TN22 *Security Agreements for Interconnected Systems* Section 4A & 4B states that:

System owners should use NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, as a guide for planning, establishing, maintaining, and terminating interconnections between SI systems and non-SI systems.

Prior to connecting the systems the system owner should prepare two documents:

- A MOU defining the responsibilities of the various organizations in establishing, operating and securing the Interconnection. This document should not contain technical details. Appendix A of the Tech Note contains a sample of this document.
- An ISA containing a statement of requirements and the system technical and security controls required for the interconnection. Appendix B of the Tech Note contains a sample of this document.

NIST SP 800-47 *Security Guide for Interconnecting Information Technology Systems*, Section 2 Background, states that:

It is critical, therefore, that both parties learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. It also is critical that they establish an agreement between themselves regarding the management, operation, and use of the interconnection and that they formally document this agreement. The agreement should be reviewed and approved by appropriate senior staff from each organization.

Federal policy requires federal agencies to establish interconnection agreements. Specifically, OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting their IT systems to other systems, based on 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 it should be included in the organization's system security plan.

Section 3.5, Step 5: The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide by the agreement, based on the team's review of all relevant technical, security, and administrative issues (Section 3.4 above). Two documents may be developed: an ISA and an MOU/A. Because the ISA and the MOU/A may contain sensitive information, they should be stored in a secure location to protect against theft, damage, or destruction. If copies are stored electronically, they should be protected from unauthorized disclosure or modification. An ISA development guide and sample are provided in Appendix A, and an MOU/A development guide and sample are provided in Appendix B.

We note that over the past couple of years the Institution has attempted to establish an interconnection agreement with NFC. We were informed that an interconnection agreement between NFC and the Institution was prepared and OCIO awaits the final signed copies from NFC.

### **Recommendation**

5. We recommend that the CIO formalize the Interconnection Security Agreement and establish the Memorandum of Understanding between the Institution and the National Finance Center of the U.S. Department of Agriculture in accordance with Institution policy and NIST guidance.

## **SUMMARY OF MANAGEMENT RESPONSE**

Management's September 7, 2007, response to our draft report concurred with our findings and recommendations. Management implemented improved user account authorization procedures for new account requests and requests for account changes. By June 2008, OCIO will ensure that all current users provide approved access forms. The CIO also agreed to strengthen its controls over segregation of duties as well as database logging and system monitoring by early 2008. In addition, OCIO has signed and submitted to the National Finance Center for their signature a Memorandum of Understanding and Interconnection Security Agreement. Finally, by April 30, 2008, OCIO agreed to establish Institution-wide baselines and document any deviations in HRMS baselines.

We include the full text of management's response in the Appendix to this report.

## **OFFICE OF THE INSPECTOR GENERAL COMMENTS**

Management has planned and taken actions that are responsive to our recommendations, and we consider them resolved. Regarding recommendation four, we urge OCIO to establish Smithsonian-wide baselines as soon as practicable because of the sensitivity of data contained in the Institution's systems and the widespread baseline weaknesses that we have identified in our FISMA-related reports.

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

## Appendix – Management Response



Smithsonian Institution

Office of the Chief Information Officer

Date September 7, 2007

To A. Sprightly Ryan, Inspector General

From Ann Speyer, Chief Information Officer   
James D. Douglas, Director, Office of Human Resources

cc Gregory Bettwy, Associate Director, Office of Human Resources  
Bruce Daniels, Director, IT Security and Smithsonian Computer Security Manager  
Deron S. Burba, Director, Systems Modernization  
Curtis Lutz, Manager, Human Resources and Administrative Division

Subject Management Response to Draft Report on the Fiscal Year 2007 Human Resource Management Systems (HRMS) Audit, Number A-07-06.

Attached please find our Management Response to the draft audit report issued on August 22, 2007.

380 Herndon Parkway, MRC 1010  
Herndon, VA 20170-4881  
202.633.2750 Telephone  
202.633. 6375 Fax

## Summary of Management's Response

We find the facts contained in the report accurate. Our responses to the individual recommendations and planned actions follow.

### **Recommendation 1: User Access Request Procedures are Not Implemented**

We recommend that the CIO enforce the Institution and HRMS-specific access control policy which requires an approved ERP HRMS access request form be submitted prior to granting new users access to HRMS. In addition, all current users who do not have an approved access request form on file should be required to complete the form.

We concur with the recommendation. As of January 1<sup>st</sup>, 2007, we began requiring all new account requests and all requests for account changes to be accompanied by a signed security form. In addition, we added a section containing a confidentiality / non-disclosure agreement to the HRMS security form. We will begin reviewing the list of current users who do not have a form on file and, starting October 1<sup>st</sup>, we will request signed forms from those users who do not have a form on file, using a phased approach. For this effort, we expect a completion date of June 29<sup>th</sup>, 2008. For those users who do not comply with the request during their phase, their accounts will be locked and review for deletion after a 30 day grace period. -- User accounts used solely for the purpose of completing online competency assessments will continue to be done on a mass approval by the Office of Human Resources (OHR).

### **Recommendation 2: Segregation of Duty Controls Need Improvement**

We recommend that the CIO identify, document, and implement segregation of duty controls for sensitive administrative and system support functions. Management should document in the system security plan those activities that need to be segregated.

We concur with the recommendation. We will update the system security plan to identify those activities that should be segregated. Based upon the identified segregated activities, we will review the roles of the existing staff performing those activities. If the roles can be separated among the existing staff, roles will be reassigned. For those where the roles cannot be separated a waiver will be obtained and exceptions documented in the security plan. We plan a completion date of January 31<sup>st</sup> 2008.

### **Recommendation 3: Database Logging and Monitoring Controls are Inadequate**

We recommend that the CIO enforce Institution policy and procedures requiring the weekly review of logs and monthly submission of appropriately detailed management reports to OCIO.

We concur with the recommendation. We will compile a list of logs upon a review of Institution's policy and procedures. Based upon the compiled list of logs we will identify the responsible individual and institute a weekly log review and monthly submission process for HRMS. We plan a completion date of March 31, 2008.

**Recommendation 4: Baseline Configurations are Not Documented**

We recommend that the CIO document final baselines for the HRMS operating system and database after determining what Institution wide baselines will be adopted. In addition, as part of installing the baselines, OCIO should specifically note where suggested security settings have not been implemented for valid business purposes.

We concur with the recommendation. Once OCIO establishes the Institutional wide baselines, we will compare HRMS baselines against the OCIO baselines and document any deviations. We plan a completion date April 30<sup>th</sup>, 2008.

**Recommendation 5: Information System Connections are Not Formally Authorized**

We recommend that the CIO formalize the Interconnection Security Agreement and establish the Memorandum of Understanding between the Institution and the National Finance Center of the U.S. Department of Agriculture in accordance with Institution policy and NIST guidance.

We concur with the recommendation. OCIO has signed and submitted to NFC for their signature a Memorandum of Understanding and Interconnection Security Agreement. We plan a completion date of November 30th, 2007, to have a signed copy by both the Smithsonian and National Finance Center. -- The interconnection between the Smithsonian and NFC predates the FISMA requirement for an Interconnection Security Agreement.