




**U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION**  
**P.O. Box 18858**  
**Washington, DC 20036-8858**

Office of  
Inspector General

September 30, 2005

**MEMORANDUM**

**TO** : Sallie Hsieh, Director  
Office of Information Technology

**FROM** : Aletha L. Brown   
Inspector General

**SUBJECT** : Final Report of OIG Report, No. 03-06-MIS,  
Assessment: EEOC Integrated mission System

Attached is the Office of Inspector General (OIG) final report on the above subject matter. We appreciate your assistance and cooperation in conducting this review.

Thank you for your draft report comments. They resulted in several changes to the report. Your comments are included, in their entirety, as Appendix I. If you have any questions regarding the final report, please contact Gregory Frazier, Management Analyst, at 663-4373 or [Gregory.Frazier@eeoc.gov](mailto:Gregory.Frazier@eeoc.gov).

Thank you again for your assistance and cooperation during our assessment.

Attachment

c: Angelica Ibarguen, Director  
Office of Human Resources

Jeffrey Smith, Director  
Office of Chief Financial Officer

**OFFICE OF INSPECTOR GENERAL**  
**Assessment**  
**Equal Employment Opportunity Commission - Integrated Mission System**  
**OIG Report Number: 03-06-MIS**  
**Sensitive Document**  
**Final Report**

## **Introduction**

The *Federal Information Security Management Act (FISMA)* of FY-2002 requires that every year each agency perform an independent evaluation of the information security program and practices of that Agency to determine the effectiveness of the program and practices. Under this Act, the Inspector General, or independent external auditor as determined by the Inspector General, shall test the effectiveness of information security policies, procedures, and practices of a representative subset of agency systems.

*FISMA* also requires that the *National Institute of Science and Technology (NIST)*: (1) develop standards, guidelines, and associated methods and techniques for information systems; (2) develop standards and guidelines, including minimum requirements, for information systems used or operated by an agency, or by a contractor of an agency, or other organization on behalf of an agency, other than national security systems; and (3) develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets.

One of the standards developed by *NIST* to aid agencies in performance of their information security responsibilities is the *NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems*. This special publication provides a method for agencies to determine the current status of their information security programs and, where necessary, establish a target for improvement. The guide is a compendium of documents that address information security (*such as: OMB Circular A-130, Transmittal Four, Appendix III; NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems; and Government Accountability Office, Federal Information Security Controls Audit Manual*).

## **Purpose, Scope, and Methodology**

Using the *NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems* as our primary evaluation tool, the Office of Inspector General (OIG) conducted an assessment of the Agency's Integrated Mission System (IMS). The purpose of our assessment was to test the effectiveness of information security policies, procedures, and practices used to secure IMS.

The Integrated Mission System (IMS) was designed and developed by the Equal Employment Opportunity Commission, Office of Information Technology (OIT), in consultation with the Office of Field Programs, the Office of General Counsel, the

Office of Federal Operations, and the Office of Research, Information, and Planning. IMS was deployed during FY-2003 and consolidates and replaces several EEOC database systems including the Charge Data System (CDS), the Automated Outreach System, and the Litigation Tracking System. IMS provides an integrated database application to support intake, mediation, investigation, state and local contract processing, outreach, and litigation.

In order for OIG to make its assertion regarding the completeness of IMS's security controls, we reviewed the system's risk assessment, security plan, as well as other documents relating to information security. OIG also interviewed individuals from the Office of Information Technology, Office of Human Resources and the Office of Chief Financial Officer and Administrative Services to obtain additional information about security controls that affect IMS. OIG reviewed 260 information system control items identified in the *NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems*.

OIG's primary fieldwork was performed from November 2003 through August 2004. We did followup work in January 2005. All work regarding this assessment was conducted in accordance with the *Comptroller General's Government Auditing Standards, (2003 Revision)*.

On March 30, 2005, the Office of Inspector General issued a draft report outlining findings and recommendations based upon our assessment of the Agency's Integrated Mission System. On April 18, 2005 the Office of Information Technology issued its comments concerning OIG's draft report. OIT's comments have been incorporated into this report and a copy of the OIT's comments are affixed to this report as an attachment.

## Findings and Recommendations

Overall, OIG found that the Integrated Mission System's security controls were adequate, however some improvements could be made to better secure this system. Based on the results of our assessment, the following are OIG's findings and recommendations. These findings and recommendations relate to controls referenced in the *NIST Special Publication 800-26*:

1. **Has a "Rules of Behavior" document been established and signed by users?**

### Finding

**OIT has not developed an IMS "Rules of Behavior" document that is specific to IMS and made available to every user prior to receiving access to the system and made available to every user prior to receiving authorization for access to the system.** *OMB Circular A-130, Transmittal Four, Appendix III* requires the establishment of a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities

and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules. Although the IMS Security Plan addresses behavior in general, the plan does not provide for a mechanism to ensure that all employees have been made aware, and acknowledge their awareness, of the specific “Rules of Behavior” related to IMS. *NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems* states that the rules of behavior should be specific to each system and made available to every user prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt.

Recommendation 1:

OIG recommends that the Director, Office of Information Technology develop a specific “Rules of Behavior” document, that all users<sup>1</sup> of IMS are required to read, in which they acknowledge their understanding of what they have read and sign it either electronically or manually prior to being granted access to IMS.

OIT Response

The first finding indicated for this item, “OIT has not developed an IMS Rules of Behavior document” is incorrect. OIT does have a “Rules of Behavior” document for the Integrated Mission System (IMS). It has been available through the IMS On-Line Help System since August 2003.

As part of a scheduled May 2005 IMS software release, OIT will implement a process by which users will be asked to read and electronically acknowledge their understanding of the IMS “Rules of Behavior” prior to being granted access to IMS.

OIG Response

OIG reviewed the home page for IMS, <http://imse0.eoc.gov/>, as well as, the IMS Case Private Sector Charge Management - Version 2.2.0 and Federal Complaint Management - Version 2.1.0 login pages and found no evidence of on-line help or rules of behavior prior to being granted access to IMS. We have modified the language in our finding to reflect that OIT does have a Rules of Behavior document, however it is not provided to the user prior to being granted access to IMS.

**2. Are mechanisms in place for holding users responsible for their actions?**

Finding:

**OIG found that while the IMS Security Plan addresses behavior, it does not adequately address the specific consequences concerning non-compliance. OMB Circular A-130, Transmittal Four, Appendix III** requires the establishment of a set of

---

1. This shall include all new employees, during orientation, and any current employees for whom OIT does not have a written acknowledgment on record.

rules concerning use of and behavior within the application. *The rules shall be as stringent as necessary to provide adequate security for the application and the information in it.* Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules. For example the *NIST Special Publication 18, Guide for Developing Security Plans for Information Technology Systems, Appendix A - Rules of Behavior, Major Applications* specifies that:

*Non-compliance of these rules will be enforced through sanctions commensurate with the level of infraction. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.*

Recommendation 2:

OIG recommends that the Director, Office of Information Technology place language within the IMS Security Plan that details in addition to rules of expected behavior, specific consequences of non-compliance with the guidelines.

OIT Response

Per OIG's recommendation, OIT will add the suggested wording into the applicable section of the IMS System Security Plan. The IMS "Rules of Behavior" document will likewise be modified to incorporate this wording.

OIG Response

OIG concurs.

**3. Is appropriate background screening for assigned positions completed prior to granting access to IMS?**

Finding:

**OIG found that a number of EEOC employees (federal employees and non-federal contract employees) who currently access IMS have not had an appropriate background screening prior to being granted access to IMS.** The *Government Accountability Office - Federal Information Security Controls Audit Manual (FISCAM)* states that the security plan should include policies related to the security aspects of hiring, terminating, and transferring employees and assessing their job performance. Procedures that should generally be in place include hiring procedures including contacting references; and background investigations and periodic re-investigations performed at least once every 5 years (consistent with the sensitivity of the position per criteria from the Office of Personnel Management).

Regarding background screening, *OMB Circular A-130 Transmittal Four* states, "for most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel

security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware that there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause.”

Recommendation 3:

OIG recommends that the Director, Office of Information Technology coordinate with the Director, Office of Human Resources (OHR) to identify (at minimum) those individuals (both federal as well as contracted employees) whose job functions allow them access to modify critical information or information system programming. Background screening for these employees should be conducted before the end of the fifth year of system operation or by the end of FY-2008.

OIT Response

OIT will continue to work with OHR to conduct background screening of federal employees and contractors consistent with the requirements of OMB Circular A-130 Appendix III, Part B.B.2)c). Completion of this requirement is pending available resources.

OIG Response

While OIG concurs with OIT’s response, we must stress the importance of conducting background screenings (at minimum) on those individuals (both federal as well as contracted employees) whose job functions allow them access to modify critical information or information system programming.

This will provide assurances that IMS and the information that resides in it is adequately protected against potential misuse.

**4. If encryption is used, does it meet federal standards?**

Finding:

**The encryption standard used in IMS does not meet federal encryption standards.** OIG reviewed the IMS Security Plan and found that the plan stated that traffic between the forms server client (the client desktop and browser) and the Windows NT web server is encrypted, by default, using 40-bit RC4 encryption. According to the *NIST Federal Information Processing Standards (FIPS)* there are four federally approved encryption algorithms which are AES, Triple DES, DES, Skipjack. RC4 is not an approved federal encryption standard.

Recommendation 4:

OIG recommends that the Director, Office of Information Technology change the encryption standard currently used by IMS between the forms server client (the client desktop and browser) and the Windows NT to meet an encryption standard approved

by *NIST*.

#### OIT Response

OIT is in the process of changing the IMS encryption standard to an encryption standard approved by NIST. As referenced in NIST draft publications SP800-52, the TLS protocol is the only approved protocol for protecting Federal data.

OIT implemented a TLS protocol to the Internet Explorer (IE) web browser agency-wide when all EEOC desktops were upgraded to the Microsoft XP operating system. The installed browser, IE 6.0.28, SP1, is configured with 128-bit encryption capability by default.

OIT is in the process of migrating all IMS web services from Microsoft NT 4.0 to Windows 2000 servers. According to NIST draft publication SP800-52, Apache is currently the only web application capable of meeting the RSA needs in the TLS protocol (for both clients and servers). Apache has been implemented on the IMS web servers used by EEOC. When IMS is ready to be deployed to FEPAs, the TLS protocol will be implemented on those IMS web servers to be accessed by FEPAs (via the Internet) along with implementation of Verisign certificates.

#### OIG Response

OIG concurs.

### **Conclusion and Recommendations**

During the assessment of the Integrated Mission System (IMS), OIG reviewed and tested 260 separate information system control items as described in *NIST Special Publication 800-26, Self-Assessment Guide for Information Technology Systems*. Based upon the final results of our testing, we conclude that, overall, the Office of Information Technology has adequately developed and deployed the appropriate information security controls to ensure the security of information that resides in the Agency's Integrated Mission System. To further improve OIT's ability to secure IMS from potential harm, OIG recommends that the Director, Office of Information Technology:

1. Require acknowledgment of "Rules of Behavior" prior to being granted access to IMS;
2. Develop specific consequences regarding non-compliance to stated rules of behavior; and
3. Ensure that an approved FIPS algorithm is used to encrypt Agency information.

Since the Director of OIT has no control over the Agency's Suitability Program or the funds for background investigations, OIG recommends to the Director of the Office of Human Resources and the Director of the Office of Chief Financial Officer

and Administrative Services to:

4. Conduct background screening of IMS users before the end of the fifth year of system operation or by the end of Fiscal Year 2008.

### **Audit Followup**

The Office of Management and Budget issued *Circular Number A-50, Audit Followup*, to ensure that corrective action regarding audit findings and recommendations proceed as rapidly as possible. *EEOC Order 192.002, Audit Followup Program*, implements *Circular Number A-50* and requires that for resolved recommendations, a corrective action work plan should be submitted within 30 days of the final audit report date describing specific tasks and completion dates necessary to implement audit recommendations. *Circular Number A-50* requires prompt resolution and corrective action on audit recommendations. Resolution should be made within six months of final report issuance.



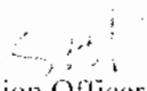


U.S. EQUAL EMPLOYMENT OPPORTUNITY COMMISSION  
Washington, D.C. 20507

APR 18 2005

MEMORANDUM

**TO:** Aletha L. Brown  
Inspector General

**FROM:** Sallie T. Hsieh   
Chief Information Officer

**SUBJECT:** Comments on OIG Report Number: 03-06-MIS, Assessment EEOC – Integrated Mission System (Draft Document)

The Office of Information Technology (OIT) is providing the comments below on the above referenced draft report.

Recommendations:

1. **OIG recommends that the Director, OIT develop a specific “Rules of Behavior” document, that all users of the IMS are required to read, in which they acknowledge their understanding of what they have read and sign it either electronically or by paper prior to being granted access to IMS.**

The first finding indicated for this item, “*OIT has not developed an IMS Rules of Behavior document*” is incorrect. OIT does have a “Rules of Behavior” document for the Integrated Mission System (IMS). It has been available through the IMS On-Line Help System since August 2003.

As part of a scheduled May 2005 IMS software release, OIT will implement a process by which users will be asked to read and electronically acknowledge their understanding of the IMS “Rules of Behavior” prior to being granted access to IMS.

2. **OIG recommends that the Director, OIT place language within the IMS Security Plan that details in addition to rules of expected behavior, specific consequences of non-compliance with the guidelines.**

Per OIG’s recommendation, OIT will add the suggested wording into the applicable section of the IMS System Security Plan. The IMS “Rules of Behavior” document will likewise be modified to incorporate this wording.

3. **OIG recommends that the Director, OIT coordinate with the Director, Office of Human Resources (OHR) to identify (at a minimum) those individuals (both federal as well as contracted employees) whose job functions allow them access to modify critical**

Office of Information Technology

||||| Phone (202) 663-4447 ||||| FAX (202) 663-4451 ||||| TTY (202) 663-7193 ||||| Help Desk (202) 663-4767 |||||||

**information or information system programming. Background screening for these employees should be conducted before the end of the fifth year of system operation.**

OIT will continue to work with OHR to conduct background screening of federal employees and contractors consistent with the requirements of OMB Circular A-130 Appendix III, Part B.B.2)c). Completion of this requirement is pending available resources.

- 4. OIG recommends that the Director, OIT change the encryption standard currently used by IMS between the forms server client (the client desktop and browser) and the Windows NT to meet an encryption standard approved by NIST.**

OIT is in the process of changing the IMS encryption standard to an encryption standard approved by NIST. As referenced in NIST draft publication SP800-52, the TLS protocol is the only approved protocol for protecting Federal data.

OIT implemented a TLS protocol to the Internet Explorer (IE) web browser agency-wide when all EEOC desktops were upgraded to the Microsoft XP operating system. The installed web browser, IE 6.0.28, SP1, is configured with 128-bit encryption capability by default.

OIT is in the process of migrating all IMS web services from Microsoft NT 4.0 to Windows 2000 servers. According to the NIST draft publication SP800-52, Apache is currently the only web application capable of meeting the RSA needs in the TLS protocol (for both clients and servers). Apache has been implemented on the IMS web servers used by EEOC. When IMS is ready to be deployed to FEPA's, the TLS protocol will be implemented on those IMS web servers to be accessed by FEPA's (via the Internet) along with implementation of VeriSign certificates.

Should you have any questions or need additional information, please contact Pierrette McIntire or Calvin Loving of OIT.

cc: Pierrette McIntire  
Calvin Loving