



US OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

**FY 2007
FEDERAL INFORMATION SECURITY
MANAGEMENT ACT
FOLLOW-UP AUDIT**

Report No. 4A-CI-00-07-008

Date: 09/18/2007

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905); therefore, while this audit report is available under the Freedom of Information Act, caution needs to be exercised before releasing the report to the general public.

AUDIT REPORT

U.S. OFFICE OF PERSONNEL MANAGEMENT

FY 2007

FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOLLOW-UP AUDIT

WASHINGTON, D.C.

Report No. 4A-CI-00-07-008

Date: 09/18/2007



Michael R. Esser
Assistant Inspector General
for Audits

EXECUTIVE SUMMARY

U.S. OFFICE OF PERSONNEL MANAGEMENT

FY 2007

FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOLLOW-UP AUDIT

WASHINGTON, D.C.

Report No. 4A-CI-00-07-008

Date: 09/18/2007

This final audit report discusses the results of a follow-up audit of the U.S. Office of Personnel Management's (OPM) fiscal year (FY) 2007 compliance with the Federal Information Security Management Act (FISMA), as well as OPM's information technology security policy. As part of our FY 2006 FISMA audit, we audited the information technology security controls of four of OPM's major applications:

- Fingerprint Transaction System (FTS)
- OPM Personnel Investigations Processing System (PIPS) Imaging System (OPIS)
- e-Individual Retirement Record (e-IRR)
- Human Resources Historical Data Warehouse (HRHDW)

In addition, the FY 2006 FISMA follow-up audit indicated that the following OPM major applications had outstanding audit recommendations from the FY 2005 and FY 2004 FISMA audits:

- Enterprise Human Resources Integration Data Warehouse (EHRI)
- USA Jobs
- PIPS Financial Interface System (PFIS)
- Electronic Questionnaire for Investigations Processing (e-QIP)
- Benefits Financial Management System (BFMS)

This report addresses the progress that each of the program offices have made in addressing the recommendations made in our prior audit reports. Our conclusions and recommendations are detailed in the “Results” section of this report.

The results of our audit are summarized below:

- HRHDW has been officially decommissioned and is no longer included in the OPM IT Inventory and Security Status List.
- The Office of the Inspector General (OIG) audited the IT security controls of FTS in FY 2006 and issued report number 4A-IS-00-06-021 with seven audit recommendations. As of September 2007, six recommendations remain outstanding (the OIG recommendations have not been implemented).
- The OIG audited the IT security controls of OPIS in FY 2006 and issued report number 4A-IS-00-06-024 with four audit recommendations. As of September 2007, all recommendations have been implemented.
- The OIG audited the IT security controls of e-IRR in FY 2006 and issued report number 4A-RI-00-06-022 with four audit recommendations. As of September 2007, all recommendations have been implemented.
- The OIG audited the IT security controls of EHRI in FY 2005 and issued report number 4A-OD-00-05-013 with 10 audit recommendations. Nine of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006. As of September 2007, the one outstanding recommendation has not yet been implemented.
- The OIG audited the IT security controls of USA Jobs in FY 2005 and issued report number 4A-OD-00-05-024 with 18 audit recommendations. Seventeen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006. As of September 2007, the one outstanding recommendation has also been implemented.
- The OIG audited the IT security controls of e-QIP in FY 2005 and issued report number 4A-IS-00-05-026 with 20 audit recommendations. Sixteen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006, and four remained outstanding. As of September 2007, these four recommendations remain outstanding.
- The OIG audited the IT security controls PFIS in FY 2005 and issued report number 4A-CF-00-05-025 with 20 audit recommendations. Nineteen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006, and one remained outstanding. In addition, the FY 2006 follow-up audit included one additional recommendation for PFIS. As of September 2007, the original recommendation remained outstanding, and the FY 2006 recommendation had been implemented.
- The OIG audited the IT security controls of BFMS in FY 2004 and issued report number 4A-CF-00-04-077 with 15 audit recommendations. Fourteen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006. As of September 2007, the one outstanding recommendation has also been implemented.

Contents

	<u>Page</u>
Executive Summary	i
Introduction and Background	1
Objectives	2
Scope and Methodology	2
Compliance with Laws and Regulations.....	4
Results.....	5
I. Human Resource Historical Data Warehouse.....	5
II. Fingerprint Transaction System.....	5
III. OPM PIPS Imaging System.....	10
IV. Electronic Individual Retirement Record	12
V. Enterprise Human Resource Integration Data Warehouse	13
VI. USA Jobs	14
VII. Electronic Questionnaire for Investigations Processing	15
VIII. PIPS Financial Interface System.....	20
IX. Benefits Financial Management System.....	21
Major Contributors to This Report	22
APPENDIX: Center for Information Services and Chief Information Officer’s September 5, 2007 response to the draft audit report, issued August 16, 2007.	

Introduction and Background

On December 17, 2002, the President signed into law the E-Government Act (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). FISMA requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies.

FISMA requires that the Office of the Inspector General (OIG) perform an audit of information technology (IT) security controls of the agency's systems on a rotating basis. As part of our Fiscal Year (FY) 2006 FISMA audit, we audited the IT security controls of four of the Office of Personnel Management's (OPM) major applications:

- Fingerprint Transaction System (FTS) - *Report No. 4A-IS-00-06-021*;
- OPM Personnel Investigation Processing System (PIPS) Imaging System (OPIS) - *Report No. 4A-IS-00-06-024*;
- Electronic Individual Retirement Record (e-IRR) - *Report No. 4A-RI-00-06-022*; and
- Human Resources Historical Data Warehouse (HRHDW) - *Report No. 4A-CA-00-06-023*

In addition, the FY 2006 FISMA follow-up audit indicated that the following OPM major applications had outstanding audit recommendations from the FY 2005 and FY 2004 FISMA audits:

- Enterprise Human Resources Integration Data Warehouse (EHRI) – *FY 2005 Report No. 4A-OD-00-05-013*;
- USA Jobs – *FY 2005 Report No. 4A-OD-00-05-024*;
- Electronic Questionnaire for Investigations Processing (e-QIP) – *FY 2005 Report No. 4A-IS-00-05-026*;
- PIPS Financial Interface System (PFIS) – *FY 2005 Report No. 4A-CF-00-05-025*; and
- Benefits Financial Management System (BFMS) – *FY 2004 Report No. 4A-CF-00-04-077*.

This audit report details our follow-up of the outstanding recommendations from each of the audits listed above, with the exception of the HRHDW, which is no longer an active OPM major application.

In conducting the audit, we applied security standards established by OPM's Center for Information Services and Chief Information Officer (CIS/CIO). These IT security policies and procedures are designed to assist program office officials in developing and documenting IT security practices that are in substantial compliance with FISMA, as well as OMB regulations and the National Institute of Standards and Technology (NIST) guidance.

In the original audit of these applications, we identified areas where IT security controls could be improved and made corresponding recommendations. For this follow-up FISMA audit, we evaluated the progress that the various program offices have made in implementing our recommendations for improving their IT security controls.

The “Results” section of this report documents the prior year recommendations; summarizes the actions taken by the program office in implementing our recommendations; highlights our evaluation of the actions taken by the program office; and offers an updated recommendation, where appropriate. We discussed the results of this follow-up audit at an exit conference and in a draft report.

Objectives

Our overall objective was to perform a follow-up evaluation of OPM’s security program and practices, as required by FISMA. This included evaluating the completion progress of recommendations made in prior FISMA reports for FTS, OPIS, e-IRR, HRHDW, EHRI, USA Jobs, e-QIP, PFIS, and BFMS.

Specific objectives:

- (1) Verify that each program office established Plans of Action and Milestones (POA&M) for each of the prior FISMA audit recommendations.
- (2) Verify that each program office is meeting scheduled completion dates as listed in their respective POA&Ms.
- (3) Review corrective actions related to weaknesses identified in the prior audit reports.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered program office FISMA compliance efforts through September 2007.

To accomplish our audit objectives, we interviewed OPM officials responsible for the security of the Agency’s information systems. We reviewed appropriate OPM IT policies and procedures; Federal laws; OMB policies and guidance; and NIST guidance; as well as analyzed various documents provided by OPM staff.

We considered the internal control structure for various OPM systems in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. Accordingly, we obtained an understanding of the internal controls for these various systems through interviews and observations, as well as inspection of various documents, including information technology and other related organizational policies and procedures. This understanding of these systems’ internal controls was used to evaluate the degree to which the appropriate internal controls were designed and implemented.

Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the system of internal controls for these various systems taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy;
- OPM IT Security Program Plan;
- OMB Circular A-130, Appendix III, “Security of Federal Automated Information Resources”;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- NIST Special Publication (SP) 800-12, “An Introduction to Computer Security”;
- NIST SP 800-18 Revision 1, “Guide for Developing Security Plans for Federal Information Systems”;
- NIST SP 800-26, “Self Assessment Guide for Information Technology Systems”;
- NIST SP 800-30, “Risk Management Guide for Information Technology Systems”;
- NIST SP 800-34, “Contingency Planning Guide for IT Systems”;
- NIST SP 800-37, “Guide for Security Certification and Accreditation of Federal Information Systems”;
- NIST SP 800-53, “Recommended Security Controls for Federal Information Systems”;
- NIST SP 800-60, “Guide for Mapping Types of Information and Information Systems to Security Categories”;
- Federal Information Processing Standards Publication 199, “Standards for Security Categorization of Federal Information and Information Systems”; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

As appropriate, we conducted compliance tests using judgmental sampling to determine the extent to which established controls and procedures are functioning as required.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. Our audit was conducted from May through September 2007 in OPM’s Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether program offices' practices were consistent with applicable standards. While generally compliant, with respect to the items tested, program offices were not in complete compliance with all standards, as described in the "Results" section of this report.

Results

This section details the progress that each of the program offices have made in addressing our prior FISMA audit report recommendations. For each prior recommendation that remains outstanding, we have summarized the action taken by the program office in implementing our recommendation; highlighted our evaluation of the action taken by the program office; and offered an updated recommendation, where appropriate. Please refer to the original reports for complete details concerning each of the unresolved recommendations.

I. Human Resource Historical Data Warehouse

On May 1, 2006 the Human Resource Historical Data Warehouse system was officially decommissioned and is no longer included in the OPM IT Inventory and Security Status List.

II. Fingerprint Transaction System

The FTS allows for the electronic scanning of fingerprint images so that agencies can conduct electronic searches of these images. OPM's Federal Investigative Services Division (FISD) has been designated with ownership of FTS. The OIG audited the IT security controls of this system in FY 2006 and issued report number 4A-IS-00-06-021 with seven audit recommendations. As of September 2007, six of the recommendations remain outstanding.

a. FY 2006 Recommendation

We recommend that FISD update the FTS Information System Security Plan (ISSP) to identify the current Designated Security Officer (DSO) and system owner and include their contact information.

FY 2007 Status

In 2006, FISD concurred with this recommendation and listed it as an action item on the system's POA&M.

As of September 2007, the recommendation remains on the FTS POA&M with a status of "Pending" and a target completion date of December 30, 2007.

FY 2007 Recommendation 1

We continue to recommend that FISD update the FTS ISSP to identify the current DSO and system owner and include their contact information.

FY 2007 FISD Response:

"FISD concurs with your recommendation. The revised FTS Contingency Plan with the requested revisions for the FTS system owner, and Designated Security Officer have been added. The document is attached for your review and consideration."

OIG Reply:

The updated FTS contingency plan addresses the OIG's recommendation. No further action is required at this time.

b. FY 2006 Recommendation

We recommend that FISD work with the Network Management Group (NMG) to ensure that changes to the FTS operating system follow established configuration management procedures and are fully documented, tracked, tested, and approved.

FY 2007 Status

In FY 2006, FISD stated that "The CIO/CIS has identified a new [change management] product called Professional that has the ability to integrate, document, track, test and approve both application and operating system changes. However, CIO/CIS does not have the environment for this system and can not provide a date for completion. Therefore, FISD has negotiated to expand the development Configuration Management System (CMS) currently used by BWXT to include the test and production environment and provide access and use by NMG for this system. These modifications and environment will be completed by August 30, 2006."

As of September 2007, the OIG has not received any documentation indicating that FISD has implemented this recommendation. The recommendation remains on the FTS POA&M with a status of "Pending". However, the target completion date of June 30, 2007 has passed.

FY 2007 Recommendation 2

We continue to recommend that FISD work with the NMG to ensure that changes to the FTS operating system follow established configuration management procedures and are fully documented, tracked, tested, and approved.

FY 2007 FISD Response:

"CIS and FISD have implemented separate configuration change boards that document, review, and formally approve configuration management changes to FTS. These boards are both operational as of 2007. FISD concurs with this recommendation and will continue to work with NMG to further expand the documentation, testing and approval of changes to FTS."

OIG Reply:

We recommend that FISD provide the OIG with documentation supporting its efforts in improving the FTS change management process. The FY 2006 recommendation will remain outstanding until such documentation is received.

c. FY 2006 Recommendation

We recommend that FISD identify personnel with significant security responsibilities for FTS and ensure that each receives appropriate security training.

FY 2007 Status

In FY 2006, FISD stated that they have “identified personnel with significant security responsibilities for FTS, which include contractor personnel under the CIO/CIS. FISD will ensure their personnel and contractors under their responsibility are trained and have requested that CIO/CIS personnel and contractors receive the appropriate security training by September 30, 2006.”

As of September 2007, the OIG has not received any documentation indicating that FISD has implemented this recommendation. The recommendation remains on the FTS POA&M with a status of “Pending”. However, the target completion date of March 31, 2007 has passed.

FY 2007 Recommendation 3

We continue to recommend that FISD identify personnel with significant security responsibilities for FTS and ensure that each receives appropriate security training.

FY 2007 FISD Response:

“FISD has identified personnel with significant security responsibility for FTS and obtained a listing of contractor personnel (BWXT) and their respective security related training. FISD concurs with this recommendation and will work to further expand the specialized security training with new personnel that have joined FISD.”

OIG Reply:

We recommend that FISD provide the OIG with documentation supporting its efforts in ensuring appropriate security training for FISD personnel. The FY 2006 recommendation will remain outstanding until such documentation is received.

d. FY 2006 Recommendation

We recommend that FISD document and maintain on file authorizations that specify the authorized privileges for each FTS user. In addition, we recommend that FISD periodically verify that only authorized users have access to FTS by reviewing user authorization forms and comparing to access lists.

FY 2007 Status

In FY 2006, FISD stated that they “will implement a system for new users by December 15, 2006, and integrate the existing population into the system by April 1, 2007. In addition, FISD will incorporate in our annual review a comparison of user access rights with the documented privileges assigned to a population of users.”

As of September 2007, the OIG has not received any documentation indicating that FISD has implemented this recommendation. The recommendation remains on the FTS POA&M with a status of “Pending”. However, the target completion date of June 30, 2007 has passed.

FY 2007 Recommendation 4

We continue to recommend that FISD document and maintain on file authorizations that specify the authorized privileges for each FTS user. In addition, we recommend that FISD periodically verify that only authorized users have access to FTS by reviewing user authorization forms and comparing to access lists.

FY 2007 FISD Response:

“Through the Interconnectivity Security Agreement (ISA) Management Program within FISD, we have required each new federal agency to document their users and have a management official authorize their official use of FTS. FISD maintains these documents. Moreover, if users do not access the system within a 120 day cycle time, their accounts are deactivated and must formally be reauthorized for access. FISD concurs with this recommendation and will work with the CIS to strengthen our ability to validate that only authorized users have access to FTS by reviewing authorization forms and comparing access lists. The SF 1665 Automation Project will further support this initiative once implemented in 2008.”

OIG Reply:

We recommend that FISD provide the OIG with documentation supporting its efforts to maintain user authorization forms and validate that only authorized users have access to FTS. The FY 2006 recommendation will remain outstanding until such documentation is received.

e. **FY 2006 Recommendation**

We recommend that FISD update the system to comply with the following OPM recommended and required settings:

- a. A session lockout feature after 10 minutes of inactivity;
- b. A password reuse setting of at least six password changes;
- c. A requirement to change passwords every 60 days; and
- d. A control that limits concurrent sessions to one for each user.

FY 2007 Status

In FY 2006, FISD stated that they “will update the system to comply with the recommendations on the platforms that are applicable in the FTS distributed environment by December 31, 2006.”

As of September 2007, the OIG has not received any documentation indicating that FISD has implemented this recommendation. The recommendation remains on the

FTS POA&M with a status of “Pending”. However, the target completion date of June 30, 2007 has passed.

FY 2007 Recommendation 5

We continue to recommend that FISD update the system to comply with the settings listed above.

FY 2007 FISD Response:

“For the system platforms where the controls are applicable, the modifications have been made. We are working with CIS to validate that all controls have been appropriately modified and that this will carry over with the new implementation of FTS in 2008. FISD concurs with this recommendation.”

OIG Reply:

We recommend that FISD provide the OIG with documentation supporting its efforts to modify system settings in accordance with the FY 2006 audit recommendation. The FY 2006 recommendation will remain outstanding until such documentation is received.

f. FY 2006 Recommendation

We recommend that FISD ensure that for the planned FY 2006 re-Certification and Accreditation (C&A) of FTS:

- The certification statement is authorized promptly by a certification agent who is independent from the system;
- The certification package is provided to the CIS/CIO for review and recommendation before accreditation;
- The certification package with CIS/CIO review and accreditation recommendation is provided to the Designated Accreditation Authority (DAA); and
- The DAA thoroughly evaluates this package before authorizing the system’s continued operation.

FY 2007 Status

Although FISD officials indicated that they would re-C&A FTS in FY 2006, the OIG has not been provided with evidence that this has occurred. The system continues to operate under the FY 2005 C&A.

As of September 2007, the recommendation remains on the FTS POA&M with a status of “Pending” and a target completion date of December 30, 2007.

FY 2007 Recommendation 6

We continue to recommend that FISD ensure that the appropriate actions outlined above are implemented regarding the planned re-C&A of FTS.

FY 2007 FISD Response:

“FISD concurs with this recommendation and will recertify and accredit FTS with the new system implementation in 2008.”

OIG Reply:

We will follow up on FISD’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit.

g. FY 2006 Recommendation

We recommend that FISD update the FTS contingency plan to fully document the following information:

- Contact Information,
- Recovery Goals/Objectives,
- Recovery Procedures,
- Original or New Site Restoration Procedures,
- Concurrent Processing Procedures, and
- Responsible Teams.

FY 2007 Status

In FY 2006, FISD stated that they “will prepare the FTS contingency plan to document the items listed by October 31, 2006.”

As of September 2007, the recommendation remains on the FTS POA&M with a status of “Pending” and a target completion date of September 30, 2007.

FY 2007 Recommendation 7

We continue to recommend that FISD prepare the FTS contingency plan to document the items listed above.

FY 2007 FISD Response:

“FISD concurs with this recommendation. The FTS Contingency Plan will be updated to reflect the recommendations above.”

OIG Reply:

We will follow up on FISD’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit.

III. OPM PIPS Imaging System

OPIS is used to convert closed investigations files into electronic form and provides a method for OPM’s FISD to process ongoing security investigations using an electronic file folder. The system also provides the capability to share case files electronically with other Federal investigative entities and agencies.

The OIG audited the IT security controls of this system in FY 2006 and issued report number 4A-IS-00-06-024 with four audit recommendations. As of September 2007, all recommendations have been implemented.

a. FY 2006 Recommendation

We recommend that FISD update the OPIS ISSP with the system's general description and purpose and date of authorization. Furthermore, we recommend that FISD identify and include the contact information for the system's authorizing official and the individual with primary security responsibility for the system.

FY 2007 Status

The most recent version of the OPIS ISSP includes the system's general description, purpose, date of authorization, and up to date contact information for the system's authorizing official and the individual with primary security responsibility. No further action is required.

b. FY 2006 Recommendation

We recommend that FISD centrally maintain security agreements for OPIS users.

FY 2007 Status

The OIG judgmentally selected a sample of 15 of 946 OPIS users and verified their acceptance of the security agreement. The results of this sample were not projected to the entire population. We found that FISD maintains copies of the signed agreements for all users at a central location. No further action is required.

c. FY 2006 Recommendation

We recommend that FISD document and maintain user authorization forms for OPIS users. We also recommend that FISD periodically review authorization forms and compare them to access lists to ensure that only authorized users have access to the system and access privileges are appropriate.

FY 2007 Status

Access authorizations for OPIS users are documented and maintained. The OIG judgmentally selected a sample of 15 of 946 OPIS users and verified that authorization to access OPIS is documented, maintained, and periodically reviewed and compared to access lists. We also verified that authorization was provided prior to granting the user access to the system. The results of this sample were not projected to the entire population. No further action is required other than the periodic comparison of access lists to authorization forms.

d. FY 2006 Recommendation

We recommend that FISD finalize and test the OPIS IT Contingency Plan and include the following elements in the finalized version of the plan:

- contact information;
- the location of the alternate processing facility; and
- an appropriate security label.

FY 2007 Status

The current OPIS IT Contingency Plan has been finalized and tested, and includes all critical elements recommended in NIST SP 800-34, “Contingency Planning Guide for Information Technology Systems”. No further action is required.

IV. Electronic Individual Retirement Record

The e-IRR captures individual retirement record (IRR) closeout data from Federal agencies and makes this data available to users via a web-based application that can search, view, edit, and print employee IRR records.

OPM’s Center for Retirement and Insurance Services (CRIS) has been designated with ownership of e-IRR. The OIG audited the IT security controls of this system in FY 2006 and issued report number 4A-RI-00-06-022 with four audit recommendations. As of September 2007, all recommendations have been implemented.

a. FY 2006 Recommendation

We recommend that CRIS update the e-IRR ISSP with the current DSO, current system operational status, and a section detailing the system’s physical and environmental controls.

FY 2007 Status

In FY 2006, CRIS updated the ISSP with the name of the current DSO and the system’s operational status, and stated they would include the system’s physical and environmental controls when the annual review of the security controls took place.

In FY 2007, CRIS provided the OIG with the most recent version of the ISSP, which included a section detailing the system’s physical and environmental controls. No further action is required.

b. FY 2006 Recommendation

We recommend that CRIS identify personnel with significant security responsibilities for e-IRR and ensure that each receives appropriate security training.

FY 2007 Status

In FY 2006, CRIS identified personnel with significant security responsibilities; and in FY 2007, CRIS provided auditors with documentation supporting the security training completed by these individuals. No further action is required.

c. FY 2006 Recommendation

We recommend that program officials take the necessary steps to ensure that a comprehensive test of e-IRR IT security controls (including tests of management, operational, and technical controls) is conducted.

FY 2007 Status

In June 2006, the system underwent a comprehensive test of its management, operational and technical controls. The OIG was provided with the test description and a report of the test results. No further action is required.

d. FY 2006 Recommendation

We recommend that program officials take the necessary steps to ensure that an independent review of the e-IRR IT security controls is conducted.

FY 2007 Status

An independent review of the e-IRR IT security controls was conducted in June 2006. No further action is required.

V. Enterprise Human Resource Integration Data Warehouse

EHRI is a web-based system that enables comprehensive electronic personnel record keeping and analysis to support human resource management across the Federal government.

The OIG audited the IT security controls of this system in FY 2005 and issued report number 4A-OD-00-05-013 with 10 audit recommendations. Nine of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006. As of September 2007, the one outstanding recommendation has not yet been implemented.

a. FY 2005 Recommendation

We recommend that the Office of e-Government Initiatives (e-Gov) implement independent organization segments for the development and migration of system programming changes to EHRI.

FY 2007 Status

In FY 2005, EHRI stated that they have “begun planning and implementation activities with the Integrator team for the reengineering of the configuration management process. A new, independent, organizational segment has responsibility for migration of all system-programming changes to the production environment.” However, the OIG was not provided with documentation to support that an independent organizational element exists.

Furthermore, implementing an independent organizational segment is only one step of the change control process. Technical controls must also be implemented that prevent developers from accessing the production environment. Consequently, the recommendation remained outstanding.

In FY 2006, the OIG reviewed the access privileges granted to EHRI developers (integrators) and found that integrators continue to have access to the EHRI production environment, as well as the development environment. As a result, the recommendation continued to remain outstanding.

As of September 2007, this recommendation has not yet been implemented. The EHRI POA&M states that the target completion date is September 30, 2007.

FY 2007 Recommendation 8

We continue to recommend that the Human Resources Line of Business Program Management Office (the current owner of EHRI) implement independent organization segments for the development and migration of system programming changes to EHRI.

FY 2007 HRLOB Response:

“Concur. Presently the target date for the relocation of Development environment is set for October 31, 2007, and the Production environment is targeted for February 29, 2008. The current status of the Development and Production hosting relocation milestones will be updated in the next quarterly POA&M report due in December 2007.”

OIG Reply:

We will follow up on HRLOB’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit.

VI. USA Jobs

USA Jobs is a web-based system that serves as a one-stop solution for bringing Government recruiters and job seekers together. In FY 2005, e-Gov maintained ownership of this system. Monster Worldwide, Inc. (Monster) is the technology manager for USA Jobs and is currently responsible for the system’s development, operation, and maintenance.

The OIG audited the IT security controls of this system in FY 2005 and issued report number 4A-OD-00-05-024 with 18 audit recommendations. Seventeen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006. As of September 2007, the one outstanding recommendation has also been implemented.

a. FY 2005 Recommendation

We recommend that e-Gov verify that only authorized users have access to USA Jobs and maintain authorization forms for all administrative tool users, operators, developers, and recruiters with USA Jobs access.

FY 2007 Status

In FY 2005, the USA Jobs Program Office stated that they had “a system in place to verify authorized user access to USA Jobs, to include the use of administrative tool users, operators, developers and recruiters.” However, the OIG did not receive documentation to support the system verification process. As a result, we were unable to confirm compliance with this recommendation.

In the OIG’s FY 2006 follow-up of this recommendation, we found that authorization forms for recruiters and administrative tool users had been documented and approved on-line. However, authorization of operators and developers had not been documented. The Monster senior project manager indicated that Monster would try to document the authorization of USA Jobs operators and developers in the near future. As a result, the recommendation remained outstanding and was placed onto the e-Gov POA&M with an expected completion date of November 30, 2006.

In FY 2007, the OIG found that the authorization forms of operators and developers are properly documented and maintained through Web Admin, an administrative tool that allows changes and modifications to the USA Jobs system. No further action is required.

VII. Electronic Questionnaire for Investigations Processing

e-QIP is one of five e-Government initiative projects assigned to OPM. The system provides applicants and contractors a venue for filling out and submitting an electronic questionnaire for sensitive positions (SF-86). OPM’s FISS, formerly known as the Center for Federal Investigative Services (CFIS), has been designated with ownership of e-QIP.

The OIG audited the IT security controls of this system in FY 2005 and issued report number 4A-IS-00-05-026 with 20 audit recommendations. Sixteen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006, and four remained outstanding. As of September 2007, these four recommendations remain outstanding.

a. FY 2005 Recommendation

We recommend that each existing e-QIP user (administrators, operators, and developers) sign a Rules of Behavior document. The signed documents should be maintained by the system DSO.

FY 2007 Status

In FY 2005, FISD stated that “Rules of Behavior are developed and will be distributed to the appropriate administrators and operators by June 30, 2005”. FISD documented the recommendation as “complete” on the system’s POA&M.

However, in FY 2006, the OIG found that the e-QIP rules of behavior statement had not been formally accepted by e-QIP users, and FISD was still in the process of implementing automated acceptance of the e-QIP rules of behavior. Consequently, the recommendation remained outstanding. FISD did not respond to the FY 2006 follow-up draft audit report.

As of September 2007, FISD has not yet implemented this recommendation. Although the recommendation has been added to the e-QIP POA&M as an action item, the target completion date of June 30, 2006 has passed and the status is listed as “Pending”.

FY 2007 Recommendation 9

We continue to recommend that FISD require each existing user to sign the rules of behavior document. The signed rules of behavior should be maintained by the system’s DSO.

FY 2007 FISD Response:

“At the time of the initial finding, there were no rules of behavior developed for e-QIP users. The POAM item was modified when two versions of rules of behavior were developed for distribution to the agency administrators and users. Through further analysis of the e-QIP user community, FISD determined that the population of users was most diverse and vast and the best strategy to reach them was through an automated solution on the ESP Portal. The ESP Portal developers were consulted and they identified a solution that would restrict access unless users electronically sign the SF 1665 OPM User Access and e-QIP Rules of Behavior. This process was the solution selected by FISD.

Moreover, CIS is managing a comprehensive effort to automate the SF 1665 and FISD is doing the same with the rules of behavior in electronic form for e-QIP user communities. Significant delays have occurred around the implementation of the forms due to selecting electronic signature standards within the broader organization, planning, data gathering and executing the requirements for the project. The implementation is forthcoming during fiscal year 2008.

FISD also implemented Privileged User Rules of Behavior that was developed and signed by OPM administrators and operators in early 2007. This effort was supported by the Network Management Group’s Security Team. A formal request for copies of the documents was executed since CIS and not FISD is retaining them. Once we receive them, copies for review and consideration will be provided. The system DSO will also retain copies of the rules of behavior per your recommendation.

FISD concurs with the recommendation and will continue to work with ESP Portal, CIS and our agency customers to fully implement this recommendation.”

OIG Reply:

We will follow up on FISD’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit. We recommend that FISD update the e-QIP POA&M to accurately reflect the estimated timeline for implementing this recommendation.

b. FY 2005 Recommendation

We recommend that the rules of behavior statement be reviewed and accepted by new users prior to granting system access.

FY 2007 Status

In FY 2005, FISD stated that “the rules of behavior will be made available to all new system users and will require their acceptance prior to granting them system access privileges.” FISD documented the recommendation as “complete” on the system’s POA&M.

However, in FY 2006, the OIG found that the e-QIP rules of behavior statement has not been formally accepted by e-QIP users, and FISD was still in the process of implementing automated acceptance of the e-QIP rules of behavior. Consequently, the recommendation remained outstanding. FISD did not respond to the FY 2006 follow-up draft audit report.

As of September 2007, FISD has not yet implemented this recommendation. Although the recommendation has been added to the e-QIP POA&M as an action item, the target completion date of June 30, 2006 has passed and the status is listed as “Pending”.

FY 2007 Recommendation 10

We continue to recommend that the e-QIP rules of behavior statement be reviewed and accepted by new users prior to granting them access to the system.

FY 2007 FISD Response:

“FISD concurs with the recommendation and will continue to work with ESP Portal, CIS and our agency customers to fully implement this recommendation.”

OIG Reply:

We will follow up on FISD’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit. We recommend that FISD update the e-QIP POA&M to accurately reflect the estimated timeline for implementing this recommendation.

c. **FY 2005 Recommendation**

We recommend that CFIS implement technical controls to identify and authorize system users that are consistent with OPM's IT Security Policy. Alternatively, we recommend that CFIS work with the CIS/CIO to ensure that the current method used by e-QIP to identify and authenticate users provides the access controls necessary to maintain an appropriate level of security. If CFIS and the CIS/CIO agree to an alternate access control methodology, this agreement should be documented.

FY 2007 Status

In FY 2005, FISD stated that "CFIS will assess and devise a plan for implementing technical controls in accordance with NIST SP 800-18 by 6/30/05 . . ." and planned to implement controls by September 30, 2005. FISD documented this recommendation in its POA&M with a projected completion date of September 30, 2006.

In FY 2006, the OIG found that FISD continued to utilize practices inconsistent with OPM's IT Security Policy to identify and authenticate system users. Consequently, the recommendation remained outstanding, and FISD did not respond to the FY 2006 follow-up draft audit report.

In FY 2007, the e-QIP POA&M indicated that this recommendation has not yet been implemented. FISD is working with the CIS/CIO to obtain concurrence on their current identification and authentication methodology and are in the process of implementing two-factor authentication on their secure portal for e-QIP agency users. The target completion date for implementing this recommendation is December 31, 2007, and the current status is listed as "Pending".

FY 2007 Recommendation 11

We continue to recommend that FISD implement technical controls to identify and authorize system users, or to document an alternate agreement with the CIS/CIO.

FY 2007 FISD Response:

"In 2006, FISD developed and submitted a formal memorandum to CIS requesting consideration for accepting e-QIP's identification and authentication methodology of golden questions and answers. FISD received an interim waiver with the agreement that e-Authentication would be implemented on the ESP portal for e-QIP users. FISD implemented e-Authentication timely during the third quarter of 2006. The agreement further recommended the implementation of two-factor authentication. This implementation is pending based on FISD's disposition determination with smart card technology and broader e-Authentication solutions to include the step-down translator as well which utilizes two factor and steps down to level two credentials, etc. FISD concurs with this recommendation and will continue to work with the e-Authentication Federation, ESP Portal and CIS to further implement this solution based on best business practice and fiscal efficiencies for FISD."

OIG Reply:

We recommend that FISC provide the OIG with documentation supporting its efforts to address the FY 2006 audit recommendation. The FY 2006 recommendation will remain outstanding until such documentation is received. We also recommend that FISC update the e-QIP POA&M to accurately reflect the estimated timeline for implementing this recommendation.

d. FY 2005 Recommendation

We recommend that CFIS verify that only authorized users have access to e-QIP and maintain authorization forms for users, including administrators, operators, and developers.

FY 2007 Status

In FY 2005, FISC stated that “CFIS will verify that only authorized users have access to e-QIP and will maintain a file of these users”. FISC documented the recommendation as “complete” on the system’s POA&M.

In FY 2006, FISC indicated that they maintain agency activation forms for e-QIP administrators at various Federal agencies to document system authorization. However, FISC indicated that each agency would be responsible for documenting and maintaining the authorization of their respective e-QIP users. We were unable to verify if authorization forms are maintained by FISC for designated e-QIP administrators, as well as OPM users. Consequently, the recommendation remained outstanding. FISC did not respond to the FY 2006 follow-up draft audit report.

As of September 2007, FISC had not yet implemented this recommendation. Although the recommendation has been added to the e-QIP POA&M as an action item, the target completion date of June 30, 2006 has passed and the status is listed as “Pending”.

FY 2007 Recommendation 12

We continue to recommend that FISC verify that only authorized users have access to e-QIP and maintain authorization forms for all users, including administrators, operators, and developers.

FY 2007 FISC Response:

“FISC concurs with your recommendation and is working to expand the implementation.”

OIG Reply:

We will follow up on FISC’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit. We recommend that FISC update the e-QIP POA&M to accurately reflect the estimated timeline for implementing this recommendation.

VIII. PIPS Financial Interface System

PFIS provides a functional interface between PIPS and the Government Financial Information System (GFIS). The functions that PFIS performs include:

- Querying billing and payable information,
- Creating reports on billing and payable information,
- Sending summary billing information to GFIS, and
- Generating monthly detailed invoices.

OPM's Center for Financial Services (CFS) within the Office of the Chief Financial Officer (OCFO) has been designated with ownership of PFIS. The OIG audited the IT security controls of this system in FY 2005 and issued report number 4A-CF-00-05-025 with 20 audit recommendations. Nineteen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006, and one remained outstanding. In addition, the FY 2006 follow-up audit included one additional recommendation for PFIS. As of September 2007, the original recommendation remained outstanding, and the FY 2006 recommendation had been implemented.

a. FY 2005 Recommendation

We recommend that CFS implement appropriate audit trails. The ISSP should be updated to include a description of these audit trail mechanisms.

FY 2007 Status

In FY 2005, CFS stated that they “. . . will implement appropriate audit trails. The PFIS ISSP will be updated to include a description of these audit trail mechanisms”. CFS documented the recommendation as complete on its POA&M.

In FY 2006, we found that the ISSP had been updated with a discussion of PFIS audit trails. However, audit trails that include the type of event, when the event occurred, and the user ID associated with the event had not been implemented on the system. Furthermore, according to the PFIS database administrator, changes to the system are done through shared accounts, minimizing the effectiveness of audit trails. Consequently, the recommendation remained outstanding, and an additional recommendation to implement individual accounts for all users was added (see section **(b)**, below).

As of September 2007, this recommendation had not yet been implemented. The recommendation was included in the PFIS POA&M with a target completion date of December 31, 2007 and the status was listed as “In Process”.

FY 2007 Recommendation 13

We continue to recommend that CFS implement appropriate audit trails. Once implemented, we recommend that CFS develop a process for periodic review of user activity.

FY 2007 OCFO Response:

“Concur. This action item is being tracked on the PFIS POA&M, #2007/1.”

OIG Reply:

We will follow up on OCFO’s efforts in implementing this recommendation as part of the FY 2008 FISMA audit.

b. FY 2006 Recommendation

We recommend that CFS implement individual user accounts for all users.

FY 2007 Status

In FY 2007, the OIG reviewed a policy that provides PFIS security administrators with instructions on how to manage PFIS user accounts (including searching, viewing, creating, modifying, deleting and unlocking individual user accounts). The policy also contained screenshots indicating that individual user accounts had, in fact, been implemented. No further action is required.

IX. Benefits Financial Management System

The Benefits Financial Management System (BFMS) provides management and accounting support for the Civil Service Retirement and Disability Fund, the Federal Employees Group Life Insurance program, and the Federal Employees Health Benefits program.

The OIG audited the IT security controls of this system in FY 2004 and issued report number 4A-CF-00-04-077 with 15 audit recommendations. Fourteen of these recommendations had been implemented when the OIG initially followed up on this report in FY 2006. As of September 2007, the one outstanding recommendation has also been implemented.

a. FY 2005 Recommendation

We recommend that CFS institute an independent review of BFMS security controls during FY 2005.

FY 2007 Status

In FY 2006, the BFMS DSO indicated that they were currently undergoing an independent test of the system’s security controls and it was expected to be completed by September 4, 2006.

In FY 2007, the OIG was provided with a copy of the current report detailing the independent test of BFMS’s security controls. No further action is required.

Major Contributors to This Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [REDACTED], Group Chief
- [REDACTED], Senior Team Leader
- [REDACTED], Auditor-in-Charge
- [REDACTED], IT Auditor




Management Services
Division

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

SEP 5 2007

MEMORANDUM FOR [REDACTED]
Chief, Information Systems Audit Group

FROM: JANET L. BARNES 
Chief Information Officer

Subject: FY 2007 Federal Information Security Management Act
Follow-up Audit

Thank you for giving the program offices and the Center for Information Services the opportunity to review your Draft of a Proposed Report, Report No: 4A-CI-00-07-008, dated August 16, 2007, FY 2007 Federal Information Security Management Act Follow-up Audit. The responses are attached. Once your report is finalized, we will ensure that every recommendation that should appropriately be addressed in a POA&M is reflected in the next quarterly POA&M updates.

If you have any questions, please contact my IT Security Officer, [REDACTED] at [REDACTED]
[REDACTED]

Attachment

I. Fingerprint Transaction System

******Text from OIG draft audit report deleted by OIG******

FY 2007 Recommendation 1

We continue to recommend that FISD update the FTS ISSP to identify the current DSO and system owner and include their contact information.

FY 2007 FISD Response:

FISD concurs with your recommendation. The revised FTS Contingency Plan with the requested revisions for the FTS system owner, and Designated Security Officer have been added. The document is attached for your review and consideration.

******Text from OIG draft audit report deleted by OIG******

FY 2007 Recommendation 2

We continue to recommend that FISD work with the NMG to ensure that changes to the FTS operating system follow established configuration management procedures and are fully documented, tracked, tested, and approved.

FY 2007 FISD Response:

CIS and FISD have implemented separate configuration change boards that document, review, and formally approve configuration management changes to FTS. These boards are both operational as of 2007. FISD concurs with this recommendation and will continue to work with NMG to further expand the documentation, testing and approval of changes to FTS.

******Text from OIG draft audit report deleted by OIG******

FY 2007 Recommendation 3

We continue to recommend that FISD identify personnel with significant security responsibilities for FTS and ensure that each receives appropriate security training.

FY 2007 FISD Response:

FISD has identified personnel with significant security responsibility for FTS and obtained a listing of contractor personnel (BWXT) and their respective security related training. FISD concurs with this recommendation and will work to further expand the specialized security training with new personnel that have joined FISD.

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 4

We continue to recommend that FISD document and maintain on file authorizations that specify the authorized privileges for each FTS user. In addition, we recommend that FISD periodically verify that only authorized users have access to FTS by reviewing user authorization forms and comparing to access lists.

FY 2007 FISD Response:

Through the Interconnectivity Security Agreement (ISA) Management Program within FISD, we have required each new federal agency to document their users and have a management official authorize their official use of FTS. FISD maintains these documents. Moreover, if users do not access the system within a 120 day cycle time, their accounts are deactivated and must formally be reauthorized for access. FISD concurs with this recommendation and will work with the CIS to strengthen our ability to validate that only authorized users have access to FTS by reviewing authorization forms and comparing access lists. The SF 1665 Automation Project will further support this initiative once implemented in 2008.

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 5

We continue to recommend that FISD update the system to comply with the settings listed above.

FY 2007 FISD Response:

For the system platforms where the controls are applicable, the modifications have been made. We are working with CIS to validate that all controls have been appropriately modified and that this will carry over with the new implementation of FTS in 2008. FISD concurs with this recommendation.

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 6

We continue to recommend that FISD ensure that the appropriate actions outlined above are implemented in regards for the planned re-certification and accreditation of FTS.

FY 2007 FISD Response:

FISD concurs with this recommendation and will recertify and accredit FTS with the new system implementation in 2008.

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 7

We continue to recommend that FISD prepare the FTS contingency plan to document the items listed above.

FY 2007 FISD Response:

FISD concurs with this recommendation. The FTS Contingency Plan will be updated to reflect the recommendations above.

II. OPM PIPS Imaging System

*****Text from OIG draft audit report deleted by OIG*****

III. Electronic Individual Retirement Record

*****Text from OIG draft audit report deleted by OIG*****

IV. Enterprise Human Resource Integration Data Warehouse

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 8

We continue to recommend that the Human Resources Line of Business Program Management Office (the current owner of EHRI) implement independent organization segments for the development and migration of system programming changes to EHRI.

FY 2007 HRLOB Response:

Concur. Presently the target date for the relocation of Development environment is set for October 31, 2007, and the Production environment is targeted for February 29, 2008. The current status of the Development and Production hosting relocation milestones will be updated in the next quarterly POA&M report due in December 2007.

V. USA Jobs

*****Text from OIG draft audit report deleted by OIG*****

VI. Electronic Questionnaire for Investigations Processing

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 9

We continue to recommend that FISD require each existing user to sign the rules of behavior document. The signed rules of behavior should be maintained by the system's DSO.

FY 2007 FISD Response:

At the time of the initial finding, there were no rules of behavior developed for e-QIP users. The POAM item was modified when two versions of rules of behavior were developed for distribution to the agency administrators and users. Through further analysis of the e-QIP user community, FISD determined that the population of users was most diverse and vast and the best strategy to reach them was through an automated solution on the ESP Portal. The ESP Portal developers were consulted and they identified a solution that would restrict access unless users electronically sign the SF 1665 OPM User Access and e-QIP Rules of Behavior. This process was the solution selected by FISD.

Moreover, CIS is managing a comprehensive effort to automate the SF 1665 and FISD is doing the same with the rules of behavior in electronic form for e-QIP user communities. Significant delays have occurred around the implementation of the forms due to selecting electronic signature standards within the broader organization, planning, data gathering and executing the requirements for the project. The implementation is forthcoming during fiscal year 2008.

FISD also implemented Privileged User Rules of Behavior that was developed and signed by OPM administrators and operators in early 2007. This effort was supported by the Network Management Group's Security Team. A formal request for copies of the documents was executed since CIS and not FISD is retaining them. Once we receive them, copies for review and consideration will be provided. The system DSO will also retain copies of the rules of behavior per your recommendation. FISD concurs with the recommendation and will continue to work with ESP Portal, CIS and our agency customers to fully implement this recommendation.

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 10

We continue to recommend that the e-QIP rules of behavior statement be reviewed and accepted by new users prior to granting access to the system.

FY 2007 FISD Response:

Through further analysis of the e-QIP user community, FISD determined that the population of users was most diverse and vast and the best strategy to reach them was through an automated solution on the ESP Portal and gain support from the agency administrators with account management. The ESP Portal developers

were consulted and they identified a solution that restricts access unless users electronically sign the SF 1665 OPM User Access and e-QIP Rules of Behavior. This process was the solution selected by FISD.

Moreover, CIS is managing a comprehensive effort to automate the SF 1665 and FISD is doing the same with the rules of behavior in electronic form for the e-QIP user community. Significant delays have occurred around the implementation of the forms due to selecting electronic signature standards within the organization and planning, gathering and executing the requirements for the project. Implementation is forthcoming during fiscal year 2008.

FISD also implemented Privileged User Rules of Behavior that was developed and signed by OPM administrators and operators in early 2007. This effort was supported by the Network Management Group's Security Team. A formal request for copies of the documents was executed since CIS and not FISD is retaining them. Once we receive them, copies for review and consideration will be provided. The system DSO will also retain copies of the rules of behavior per your recommendation. FISD concurs with the recommendation and will continue to work with ESP Portal, CIS and our agency customers to fully implement this recommendation.

****Text from OIG draft audit report deleted by OIG****

FY 2007 Recommendation 11

We continue to recommend that the CFIS implement technical controls to identify and authorize system users, or to document an alternate agreement with the CIS & CIO.

FY 2007 FISD Response:

In 2006, FISD developed and submitted a formal memorandum to CIS requesting consideration for accepting e-QIP's identification and authentication methodology of golden questions and answers. FISD received an interim waiver with the agreement that e-Authentication would be implemented on the ESP portal for e-QIP users. FISD implemented e-Authentication timely during the third quarter of 2006. The agreement further recommended the implementation of two-factor authentication. This implementation is pending based on FISD's disposition determination with smart card technology and broader e-Authentication solutions to include the step-down translator as well which utilizes two factor and steps down to level two credentials, etc. FISD concurs with this recommendation and will continue to work with the e-Authentication Federation, ESP Portal and CIS to further implement this solution based on best business practice and fiscal efficiencies for FISD.

****Text from OIG draft audit report deleted by OIG****

FY 2007 Recommendation 12

We continue to recommend that FISD verify that only authorized users have access to e-QIP and maintain authorization forms for all users, including administrators, operators, and developers.

FY 2007 FISD Response:

At the time of the initial finding, there were no rules of behavior developed for e-QIP users. The POAM item was modified when two versions of rules of behavior were developed for distribution to the agency administrators and users. Through further analysis of the e-QIP user community, FISD determined that the population of users was most diverse and vast and the best strategy to reach them was through an automated solution on the ESP Portal. The ESP Portal developers were consulted and they identified a solution that would restrict access unless users electronically sign the SF 1665 OPM User Access and e-QIP Rules of Behavior. This process was the solution selected by FISD.

Moreover, CIS is managing a comprehensive effort to automate the SF 1665 and FISD is doing the same with the rules of behavior in electronic form for the e-QIP user community. Significant delays have occurred around the implementation of the forms due to selecting electronic signature standards within the broader organization, planning, data gathering and executing the requirements for the project. Implementation is forthcoming during fiscal year 2008.

FISD also implemented Privileged User Rules of Behavior that was developed and signed by OPM administrators and operators in early 2007. This effort was supported by the Network Management Group's Security Team. A formal request for copies of the documents was executed since CIS and not FISD is retaining them. Once we receive them, copies for review and consideration will be provided. The system DSO will also retain copies of the rules of behavior per your recommendation. FISD concurs with the recommendation and will continue to work with ESP Portal, CIS and our agency customers to fully implement this recommendation.

In FY 2006, FISD initiated and maintained agency activation forms for e-QIP administrators at various Federal agencies to document system authorization. FISD's strategy is that each agency would be responsible for documenting and maintaining the authorization of their respective e-QIP users. FISD is planning to work more closely with agencies to verify that authorization forms are maintained by them for designated e-QIP administrators, as well as their respective e-QIP users. FISD concurs with your recommendation and is working to expand the implementation.

VII. PIPS Financial Interface System

*****Text from OIG draft audit report deleted by OIG*****

FY 2007 Recommendation 13

We continue to recommend that CFS implement appropriate audit trails. Once implemented, we recommend that CFS develop a process for periodic review of user activity.

FY 2007 OCFO Response:

Concur. This action item is being tracked on the PFIS POA&M, #2007/1.

****Text from OIG draft audit report deleted by OIG****

VIII. Benefits Financial Management System

****Text from OIG draft audit report deleted by OIG****